HIRSCHMANN
A BELDEN BRAND

User Manual

Configuration and Administration Guide OpenBAT Family

The naming of copyrighted trademarks in this manual, even when not specially indicated, should not be taken to mean that these names may be considered as free in the sense of the trademark and tradename protection law and hence that they may be freely used by anyone.

© 2013 Hirschmann Automation and Control GmbH

Manuals and software are protected by copyright. All rights reserved. The copying, reproduction, translation, conversion into any electronic medium or machine scannable form is not permitted, either in whole or in part. An exception is the preparation of a backup copy of the software for your own use. For devices with embedded software, the end-user license agreement on the enclosed CD/DVD applies.

The performance features described here are binding only if they have been expressly agreed when the contract was made. This document was produced by Hirschmann Automation and Control GmbH according to the best of the company's knowledge. Hirschmann reserves the right to change the contents of this document without prior notice. Hirschmann can give no guarantee in respect of the correctness or accuracy of the information in this document.

Hirschmann can accept no responsibility for damages, resulting from the use of the network components or the associated operating software. In addition, we refer to the conditions of use specified in the license contract.

You can get the latest version of this manual on the Internet at the Hirschmann product site (www.hirschmann.com).

Printed in Germany
Hirschmann Automation and Control GmbH
Stuttgarter Str. 45-51
72654 Neckartenzlingen
Deutschland
Tel.: +49 1805 141538

Contents

Safety instructions 21

Related Documents 23

Key 25

1 Device Roles 27

1.1 Access Point 29
1.2 WLAN Bridge (point-to-point) 30
1.3 WLAN Bridge Relay 32
1.4 WLAN Distribution Point - (Point-to-Multipoint) 33
1.5 WLAN Client 34
1.6 WLAN Roaming Clients 35

2 Configuration Tools 37

2.1 Startup Behavior 39
2.2 Online versus Offline Configuration 40
2.3 Downloading the Configuration File 41

3 Configuring the Device 43

3.1 Creating a Configuration File 44

3.2 Access Point for Multiple Wireless Clients 47
3.2.1 Creating a New Configuration File 48
3.2.2 Configuring Basic Settings 51
3.2.3 Configuring Wireless LAN Settings 59

3.3 Access Point & DHCP Server for Multiple Wireless Clients 78
3.3.1 Creating a New Configuration File 79
3.3.2 Changing the Existing Network to a Wired LAN 79
3.3.3 Create a New DHCP Wireless LAN 82

3.4 Wireless Client 85
3.4.1 Creating a New LANconfig File for a Client 85
3.4.2 Configuring Basic Settings 88
3.4.3 Configuring Wireless LAN Settings 94

3.5 WLAN Bridge: Single Subnet 105
3.5.1 Configuring the LEFT Device 105
3.5.2 Configuring the RIGHT Device 132

3.6 WLAN Bridge: Two Subnets 142
3.6.1 Creating Two LANconfig Files 143
3.6.2 Creating Two Transfer Network Entries 145
3.6.3 Routing the Transfer Networks 150

3.7 WLAN Bridge Relay: 1 Radio 155
3.7.1 Creating Three LANconfig Files 156
3.7.2 Configure the LEFT Device 161
3.7.3 Configure the MIDDLE Device 167
3.7.4 Configure the RIGHT Device 172

3.8 WLAN Bridge Relay: 2 Radios 177
3.8.1 Creating Three LANconfig Files 178
3.8.2 Configuring the MIDDLE Device 179
3.8.3 Configuring the LEFT Device 191
3.8.4 Configuring the RIGHT Device 194

4 Central WLAN Management 197

4.1 Application Examples 198
4.1.1 Managed Mode 198
4.1.2 WLAN Bridge to Access Point – Managed and Unmanaged Mixed 200

4.2 Introduction 201
4.2.1 The CAPWAP Standard 202
4.2.2 The Smart Controller Technology 202
4.2.3 Communication between Access Point and WLAN-Controller 206
4.2.4 Zero-Touch Management 209
4.2.5 Split Management 209
4.2.6 Inheritance of Parameters 209

4.3 Configuration of the WLC 212
4.3.1 General settings 212
4.3.2 Profiles 213
4.3.3 List of Access Points 218
4.3.4 Station Table (ACL Table) 222
4.3.5 Options for the WLAN-Controller 222

4.4 Configuring the Access Points 224
4.4.1 WLAN band steering 226
4.4.2 UUID Information Element for WLAN Access Points 227
4.4.3 PMK Caching in the WLAN Client Mode 229
4.4.4 Pre-authentication in WLAN Client Mode 229
4.4.5 Time-staggered Roaming for Dual-radio Client WLAN Modules 230
4.4.6 Greenfield Mode for Access Points with IEEE 802.11n 232

4.5 Related Information on General WLAN Configuration 234
4.5.1 STBC / LDPC 234
4.5.2 DFS 235

4.6 Managing the Access Points 237
4.6.1 Accepting new Access Points manually into the WLAN structure 237
4.6.2 Removing Access Points manually from the WLAN structure 241
4.6.3 Deactivating or Permanently Removing Access Points from the WLAN Structure 242
4.6.4 Managing the Access Points 243
4.6.5 Backing up the Certificates 244

4.6.6 Saving and Restoring more files of the SCEP-CA 246
4.7 Interference Detection in the Frequency Range (Spectral Scan) 249
4.7.1 Functions of the Software Module 250
4.7.2 Starting a Spectral Scan 250
4.7.3 Spectral Scan Analysis Window 254
4.8 Extended WLC Functions 258
4.8.1 Automatic Radio-Field Optimization with Hirschmann WLAN-Controllers 258
4.8.2 Central Firmware and Script Management 260
4.8.3 Checking WLAN Clients with RADIUS (MAC Filter) 265
4.8.4 Separate RADIUS Server for Each SSID 267
4.8.5 Dynamic VLAN Assignment 269
4.8.6 Load Balancing between the WLAN-Controllers 272
4.8.7 WLAN Layer-3 Tunneling 273
4.9 Application Examples 277
4.9.1 "Overlay Network": Separating Networks for Access Points without VLAN 277
4.9.2 "Layer-3 Roaming" 284
4.9.3 WLAN Controller with Public Spot 287

5 Public Spot 297

5.1 What is a Public Spot? 297
5.1.1 The Solution: (W)LAN Technology 297
5.1.2 User Authorization and Authentication 298
5.1.3 Accounting 299
5.1.4 Logging 299

5.2 Overview of the Public Spot Module 299
5.2.1 Open User Authentication (OUA) 299
5.2.2 Security in the (W)LAN 301
5.2.3 Setup Wizard for Public Spots 303
5.2.4 Wizard for Managing Users 303

5.3 Basic Configuration 304
5.3.1 Basic installation of a Public Spot for Simple Scenarios 304
5.3.2 Default Values for the Public Spot Wizard 323
5.3.3 Setting up an Administrator for Public Spot Management 325
5.3.4 Setting up Public Spot users for Simple Scenarios 327

5.4 Security Settings 332
5.4.1 Traffic Limit Option 333
5.4.2 Restricting Access to the Configuration 334

5.5 Advanced Functions and Settings 335
5.5.1 Multiple Logins 336
5.5.2 Open Access Networks (No Login) 337
5.5.3 Managing Public Spot Users Via the Web API 339
5.5.4 Clear User List Automatically 345
5.5.5 Station Monitoring 345
5.5.6 WLAN Handover of Sessions Between Devices 346
5.5.7 Authentication via RADIUS 349
5.5.8 Billing Without a RADIUS Accounting Server 352
5.5.9 Billing via RADIUS Accounting Server 352
5.5.10 Multilevel Certificates for Public Spots 354
5.5.11 Assigning Users to Individual VLANs 355

5.6 Alternative Login Methods 357
5.6.1 Overview of Authentication Modes 357
5.6.2 Independent User Authentication (Smart Ticket) 359
5.6.3 Automatic Authentication with the MAC Address 359

5.7 XML Interface 362

5.7.1 Function 362
5.7.2 Setting up the XML Interface 365
5.7.3 Analyzing the XML Interface with cURL 366
5.7.4 Commands 367
5.8 Default and Customized Authentication Pages 374
5.8.1 Available Pages 375
5.8.2 Pre-installed Default Pages 377
5.8.3 Configuration of User-defined Pages 377
5.8.4 URL Placeholder (Template Variables) 379
5.8.5 User-defined Pages Via HTTP Redirect 380
5.8.6 User-defined Pages Via Page Templates 381
5.8.7 Page Template Syntax 382
5.8.8 Page Template Identifiers 383
5.8.9 Graphics in User-defined Pages 386
5.9 Access to the Public Spot 386
5.9.1 Requirements for Logging In 386
5.9.2 Logging in to the Public Spot 388
5.9.3 Session Information 389
5.9.4 Logging out of the Public Spot 389
5.9.5 Advice and Help 390
5.10 Commonly Transmitted RADIUS Attributes 392
5.10.1 Messages to/from the Authentication Server 392
5.10.2 Messages to/from the Accounting Server 397

6 Virtual Private Networks – VPN 401

6.1 What are the Benefits of VPN? 402
6.1.1 Private IP Addresses on the Internet? 403
6.1.2 Security of Data Traffic on the Internet? 404

6.2 VPN at a Glance 407
6.2.1 VPN Application Example 407
6.2.2 VPN Functions 409

6.3 Configuration of VPN Connections 410
6.3.1 VPN Tunnel: Connection between VPN Remote Terminals 410
6.3.2 1-Click VPN for LANCOM Advanced VPN Client 412
6.3.3 Viewing VPN Rules 413
6.3.4 Manually Setting up VPN Connections 415
6.3.5 IKE Config Mode 416
6.3.6 Establishing VPN Network Relationships 418
6.3.7 Collective Establishment of Security Associations 421
6.3.8 VPN Connection Diagnostics 423

6.4 IPSec over HTTPS 424
6.4.1 Introduction 424
6.4.2 Configuring the IPSec over HTTPS Technology 424
6.4.3 Status Displays for IPSec over HTTPS Technology 427

6.5 Use of Digital Certificates 428
6.5.1 Basics 428
6.5.2 Advantages of certificates 436
6.5.3 Structure of certificates 437
6.5.4 Security 439
6.5.5 Certificates in VPN connection setup 440
6.5.6 Certificates from certificate service providers 442
6.5.7 Structure of one's own CA 443
6.5.8 Requesting a certificate with the standalone Windows CA 444
6.5.9 Exporting the certificate to a PKCS#12 file 446
6.5.10 Creating certificates with OpenSSL 449
6.5.11 Loading certificates into the Hirschmann device 452
6.5.12 Backing up and uploading certificates with LANconfig 453
6.5.13 Adjusting VPN connections to certificate support 454
6.5.14 Creating certificate-based VPN connections for LAN coupling using the Setup Wizard 461

6.5.15 Simplified network connection with certificates – pro-adaptive VPN 463
6.5.16 Requesting certificates by means of CERTREQ 465
6.5.17 Certificate revocation list - CRL 465
6.5.18 Diagnosis of the VPN certificate connections 469
6.6 Multilevel certificates for SSL/TLS 470
6.6.1 Introduction 470
6.6.2 SSL/TLS with multilevel certificates 472
6.6.3 VPN with multilevel certificates 472
6.7 Certificate enrollment via SCEP 473
6.7.1 SCEP server and SCEP client 474
6.7.2 The process sequence of a certificate distribution 474
6.7.3 Configuration of SCEP 477
6.8 Extended Authentication Protocol (XAUTH) 483
6.8.1 Introduction 483
6.8.2 XAUTH in HiLCOS 484
6.8.3 Configuration of XAUTH 484
6.9 How does VPN operate? 487
6.9.1 IPSec – the basis for VPN 487
6.9.2 Alternatives to IPSec 488
6.10 The standards behind IPSec 491
6.10.1 Modules of IPSec and their tasks 491
6.10.2 Security Associations – numbered tunnels 492
6.10.3 Encryption of the packets – the ESP protocol 492
6.10.4 Authentication – the AH protocol 495
6.10.5 Management of the keys – IKE 499
6.11 Improved phase 1 rekeying 501
6.12 Intelligent Precalculation of DH Keys 502
6.13 MPPE encryption for PPTP tunnel 503
6.13.1 Enhancements in the menu system 503

7 Security 505

7.1 A WLAN Security Overview 506
7.1.1 Basic Considerations 506
7.1.2 IEEE 802.11i /WPA2 507
7.1.3 TKIP and WPA 507
7.1.4 WEP 507
7.1.5 LEPS: LANCOM Enhanced Passphrase Security 508
7.1.6 Background WLAN Scanning 509

7.2 Securing the Configuration 510
7.2.1 Using the Check Security Settings Wizard 510
7.2.2 Passwords 511
7.2.3 Login Barring 513
7.2.4 Restricting Configuration Access Rights 513
7.2.5 Closed-network Function: Suppress SSID broadcast 517

8 Virtual LANs 519

8.1 What is a Virtual LAN? 520

8.2 Configuring VLANs 521
8.2.1 VLAN and ARF 521
8.2.2 General VLAN Settings 522
8.2.3 The Network Table 523
8.2.4 The Port Table 524

8.3 Configuring VLAN IDs 527
8.3.1 Assigning Different VLAN IDs to WLAN Clients 527
8.3.2 Special VLAN ID for DSL Interfaces 528

8.4 VLAN Tagging on Ethernet Layers 2 and 3 529
8.4.1 Introduction 529
8.4.2 Configuration of VLAN tagging on layer 2/3 530

9 LLDP 533
9.1 How it works 534
9.2 Structure of LLDP Messages 535
9.3 Supported Operating Systems 536
9.4 Configuration 537

10 Routing and WAN Connections 539

10.1 General aspects of WAN connections 540
10.1.1 Bridges for Standard Protocols 540

10.2 IP Routing 542
10.2.1 The Routing Table 542
10.2.2 Policy Based Routing 546
10.2.3 Local Routing 550
10.2.4 Dynamic Routing with IP RIP 551
10.2.5 SYN/ACK Speedup 559

10.3 Advanced Routing and Forwarding 560
10.3.1 Introduction 560
10.3.2 Definition of networks and Assignment of Interfaces 566
10.3.3 Assigning Logical Interfaces to Bridge Groups 567
10.3.4 Interface Tags for Remote Sites 568
10.3.5 Virtual Routers 570
10.3.6 NetBIOS Proxy 572

10.4 Configuring Remote Stations 574
10.4.1 Remote Site (Peer) List 574
10.4.2 Communication Layers List 576

10.5 IP Masquerading 579
10.5.1 Simple Masquerading 579
10.5.2 Inverse Masquerading 582

10.6 Demilitarized Zone (DMZ) 587
10.6.1 Assigning Networks to the DMZ 588
10.6.2 Address Checking 589
10.6.3 Unmasked Internet Access for a Server in the DMZ 589

10.7 N:N Mapping 591
10.7.1 Application Examples 592
10.7.2 Configuring Address Translation 597

10.8 Establishing Connection with PPP 600
10.8.1 The Point-to-Point Protocol (PPP) 600
10.8.2 Checking the Connection with LCP 603
10.8.3 Assignment of IP Addresses via PPP 604
10.8.4 Configuring PPP Negotiation Settings 606
10.8.5 The DEFAULT Remote Site 608
10.8.6 RADIUS authentication of PPP connections 609

10.9 PPPoE Servers 611
10.9.1 Introduction 611
10.9.2 Example Application 612
10.9.3 Configuring PPPoE 615
10.10 DSL Dial-in over PPTP 617
10.11 Automatic Configuration of WLAN P2P Connections via Serial Interfaces 619
10.12 Keep Alive: Extended Connections for Flat Rates 620
10.13 Callback Functions 621
10.13.1Callback for Microsoft CBCP 622
10.13.2Fast Callback 623
10.13.3Callback via RFC 1570 (PPP LCP Extensions) 624
10.13.4Overview of WEBconfig, Terminalprogram and Telnet 624
10.14 Operating a modem over the serial interface 626
10.14.1System Requirements 627
10.14.2Installation 627
10.14.3Configuring the serial interface for modem operation 628
10.14.4Configuring Modem Parameters 629
10.14.5Direct Entry of AT Commands 631
10.14.6Statistics 631
10.14.7Trace Output 632
10.14.8Configuring Remote Sites for V.24 WAN Interfaces 633
10.14.9Configuring a Backup Connection on the Serial Interface 634
10.14.10Contact Assignment of Modem Connectors 637
10.15 Manual Definition of the MTU 638
10.15.1Configuring the MTU 638
10.15.2Statistics 639
10.16 WAN RIP 640
10.17 The Rapid Spanning Tree Protocol 643
10.17.1Classic and Rapid Spanning Tree 644
10.17.2RSTP Improvements 645
10.17.3Configuring the Spanning Tree Protocol 646
10.17.4Status Reports for Spanning Tree 648
10.18 The Action Table 652
10.18.1Actions for Dynamic DNS 652
10.18.2Action Examples 658

10.18.3Configuring action table entries 661
10.19 Using the LAN Serial Interface 665
10.19.1Operating Modes 666
10.19.2Configuring the Serial Interface 666
10.19.3Configuring the COM Port Server 667
10.19.4WAN Device Configuration 675
10.19.5Serial Connection Status Information 676
10.19.6CPM Port Adapters 680
10.20 IGMP Snooping 681
10.20.1Introduction 681
10.20.2IGMP Snooping Operation 683
10.20.3IGMP snooping through multiple bridges 684
10.20.4Configuring IGMP Snooping 687
10.20.5IGMP Status 692

11 Configuring the Firewall 697

11.1 The Device Firewall 698
11.1.1 Tips for Configuring the Firewall 698

11.2 Firewall Configuration: LANconfig 701
11.2.1 General Firewall Parameters 701
11.2.2 Creating a New IPv4 Firewall Filter Rule 706
11.2.3 Firewall filter rule settings and actions 708
11.2.4 Applying firewall rules to FTP and IRC connections 717
11.2.5 Defining Firewall Objects 720

11.3 Configuring the IPv4 Firewall: WEBconfig and Telnet 724
11.3.1 Rules Table 724
11.3.2 Objects Table 725
11.3.3 Action Table 727

11.4 Firewall Diagnosis 728
11.4.1 The Firewall Log Table 728
11.4.2 The Filter List 730
11.4.3 The Connection List 732
11.4.4 Port Block List 733
11.4.5 Host Block List 734

11.5 Firewall Limitations 735

11.6 Combating intrusion attempts Intrusion detection 736
11.6.1 Examples of Break-in Attempts 736
11.6.2 Configuring the IDS 737

11.7 Protection from denial of service attacks 739
11.7.1 Configuring DoS Blocking 739

12 IPv6 743

12.1 IPv6 basics 743
12.1.1 Why Use IPv6-standard IP Addresses? 743
12.1.2 IP Address Structure According to the IPv6 Standard 744
12.1.3 Stages of Migration 745

12.2 IPv6 Tunneling Technologies 745
12.2.1 6in4 Tunneling 745
12.2.2 6rd Tunneling 746
12.2.3 6to4 Tunneling 747

12.3 DHCPv6 748
12.3.1 DHCPv6 Server 749
12.3.2 DHCPv6 Client 749

12.4 IPv4 VPN Tunnel via IPv6 750
12.4.1 Setup Wizard: IPv4 VPN Tunnel via IPv6 Setup 751

12.5 IPv6 Firewall 752
12.5.1 Function 752
12.5.2 Configuration 752
12.5.3 Default Entries for the IPv6 Firewall Rules 753
12.5.4 IPv6 Firewall Log Table 754

12.6 Additional Command-line Commands 757
12.6.1 IPv6 Addresses 757
12.6.2 IPv6 Prefixes 759
12.6.3 IPv6 Interfaces 759
12.6.4 IPv6 Neighbor Cache 759
12.6.5 IPv6 DHCP Server 760
12.6.6 IPv6 DHCP Client 760
12.6.7 IPv6 Route 761
12.6.8 Release IPv6 Address 761
12.6.9 Overview of Parameters 761

12.7 Enhancements to LANconfig 763
12.7.1 IPv6 configuration menu 763
12.7.2 Configuring PPP Negotiation Settings 785
12.7.3 IP Routing Tables 786
12.7.4 Separate Views for the IPv4 and IPv6 Firewalls 788
12.7.5 IPv6 DNS Hosts in the DNS List 788
12.7.6 Configuring the IPv6 Firewall Rules 788

12.8 Tutorials 807
12.8.1 Setting up IPv6 Internet Access 807
12.8.2 Setting up a 6to4 Tunnel 820

13 Quality of Service 831

13.1 QoS Objectives 832

13.2 Which packets to prioritize? 833

13.3 Configuration of QoS 834
13.3.1 Evaluating ToS and DiffServ fields 834
13.3.2 Granting Minimum Bandwidths 837
13.3.3 Configuring the send/receive direction 838
13.3.4 Reducing Packet Length 839

13.4 QoS for WLANs: IEEE802.11e (WMM/WME) 842

14 Additional Services 845

14.1 IP Address Administration via DHCP 846
14.1.1 Introduction 846
14.1.2 Configuring DHCP parameters in LANconfig 848
14.1.3 Configuring DHCP parameters via WEBconfig or Telnet 855
14.1.4 DHCP Relay Server 863
14.1.5 Configuring Clients 865
14.1.6 Checking IP Addresses in the LAN 866

14.2 Vendor class and User class identifiers 868

14.3 DNS 869
14.3.1 DNS Functions 869
14.3.2 DNS Forwarding 871
14.3.3 Configuring the DNS Server 873
14.3.4 URL Blocking 879
14.3.5 Dynamic DNS 880

14.4 Accounting 883
14.4.1 Configuring General Accounting Parameters 883
14.4.2 Configuring the Snapshot 885

14.5 Call Charge Management 886
14.5.1 Connection limits for DSL and cable modem 886

14.6 Time Server 889
14.6.1 Configuring the time server with LANconfig 889
14.6.2 Configuring the time server with WEBconfig 891
14.6.3 Configuring NTP Clients 891

14.7 Scheduled Events 895
14.7.1 CRON Jobs With Time Delay 896
14.7.2 Configuring a CRON Job 896

14.8 RADIUS 900
14.8.1 How RADIUS Works 902
14.8.2 Configuring RADIUS as Authenticator or NAS 903
14.8.3 Configuring the RADIUS Server 912

14.9 RADSEC 927
14.9.1 Configuring RADSEC in the OpenBAT device 927
14.9.2 Certificates for RADSEC 928

14.10 TACACS+ 929

14.10.1Introduction 929
14.10.2Configuring TACACS+ 931
14.10.3Configuring the TACACS+ Server 935
14.10.4Login to the TACACS+ Server 936
14.10.5TACACS+ Login via Telnet or SSH 939
14.10.6Assigning Rights Under TACACS+ 940
14.10.7Authorization Functions 940
14.11 Support from TLS 1.1 / 1.2 943

A Glossary 945

B Index 953

C General Information 963
C.1 Maintenance 964
C.2 Readers' Comments 965

D Further Support 967

Safety instructions

Important Information

Notice: Read these instructions carefully, and look at the equipment to become familiar with the device before trying to install, operate, or maintain it. The following special messages may appear throughout this documentation or on the equipment to warn of potential hazards or to call attention to information that clarifies or simplifies a procedure.

The addition of this symbol to a Danger or Warning safety label indicates that an electrical hazard exists, which will result in personal injury if the instructions are not followed.

This is the safety alert symbol. It is used to alert you to potential personal injury hazards. Obey all safety messages that follow this symbol to avoid possible injury or death.

DANGER

DANGER indicates an imminently hazardous situation which, if not avoided, **will result in** death or serious injury.

WARNING

WARNING indicates a potentially hazardous situation which, if not avoided, **can result in** death or serious injury.

CAUTION

CAUTION indicates a potentially hazardous situation which, if not avoided, **can result in** minor or moderate injury.

Related Documents

Title of the document
OpenBAT Configuration and Administration Guide
OpenBAT Installation User Manual
Reference Manual Command Line Interface OpenBAT Family
WLAN Outdoor Guide
Antenna Guide Wireless LAN Antennas of the OpenBAT family

Key

The designations used in this manual have the following meanings:

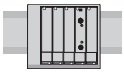
▶	List
☐	Work step
	Subheading
Link	Cross-reference with link
Note:	A note emphasizes an important fact or draws your attention to a dependency.
`Courier`	ASCII representation in user interface

Execution in the Graphical User Interface (Web-based Interface user interface)

Execution in the Command Line Interface user interface

Symbols used:

	WLAN access point
	Router with firewall
	Switch with firewall
	Router
	Switch
	Bridge

	Hub
	A random computer
	Configuration Computer
	Server
	PLC - Programmable logic controller
	I/O - Robot

1 Device Roles

Wireless local area networks (WLANs) can either extend or replace a traditional cable-based network. In some cases, a wireless LAN provides new application design possibilities, providing streamlined work flows and cost savings.

Note: Graphics displayed in the manual may differ from those displayed on your PC as a consequence of hardware and firmware revisions.

You can use the OpenBAT device in many different roles, depending upon the specific features and the requirements of your network design. These roles include:

- Access Point:
  The OpenBAT device enables Client devices to gain wireless access to a cable-based local area network.
- WLAN Bridge:
  Two OpenBAT devices provide a wireless point-to-point communication link between two typically cable-based LANs.
- WLAN Bridge Relay:
  Two or more dual-radio OpenBAT devices serve as message relay stations, providing a communication link between two typically cable-based LANs.
- WLAN Distribution Point:
  A single master OpenBAT device connects multiple slave Access Points to a central LAN in a point-to-multipoint design.

- WLAN Client:
  A OpenBAT device is designed or configured to serve as Ethernet adapter and provide a wireless communication link to a WLAN Access Point.
- WLAN Roaming Client:
  WLAN clients wirelessly connect one or more mobile units as they move between multiple WLAN access points, providing continuous, dynamic communications.

Each of these roles is briefly described below. The following chapter describes how to configure OpenBAT devices to perform each of these roles.

1.1 Access Point

The OpenBAT device can function as central Access Point, connected to multiple wireless clients. In this application example, a OpenBAT device provides client access to one or more WLANs and regulates:

– each client's rights to access the radio cell
– communications between clients
– access to networks linked to other networks

In larger scale WLAN scenarios (e.g. in companies with facilities extending between several buildings or floors), multiple Access Points can provide WLAN Clients with access to a common, shared network. The clients can roam between the different Access Points, if necessary. Such a design is commonly referred to as campus coverage because this solution has been adopted by a large number of colleges and universities to provide students and staff with network access.

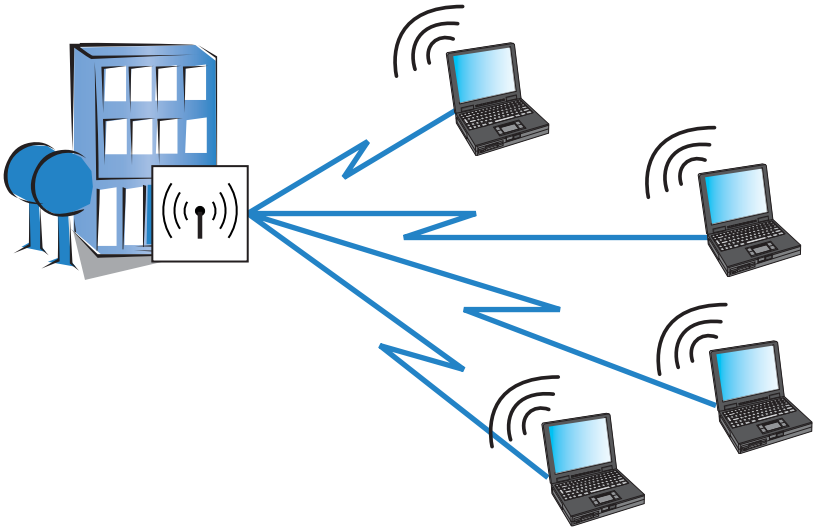


Figure 1: A single access point connected to wireless clients

1.2 WLAN Bridge (point-to-point)

Outdoor WLAN systems are especially useful for providing a point-to-point (P2P) link between two Access Points. This design makes it possible, for example, to easily integrate a remote production building into the company network using two OpenBAT devices.

Figure 2: A wireless link between two access points

You can also use a point-to-point connection to span difficult terrain (such as mountainous areas or water) to provide network access in areas where cabling would be too expensive. With a direct line of sight between the two access points and a sufficient Fresnel zone, you can bridge distances of several kilometers by this type of wireless link.

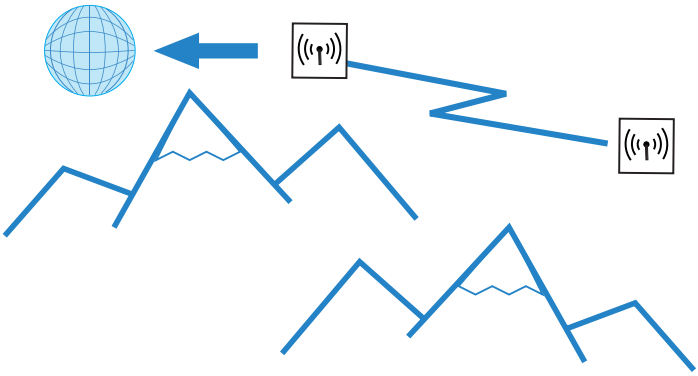


Figure 3: Point-to-point connection with a direct line of sight

1.3 WLAN Bridge Relay

Sometimes the required distance between two Access Points may exceed the maximum radio range of a wireless link. Also, physical obstacles may exist that prevent an uninterrupted line-of-sight connection between two Access Points.

In these cases, you can connect the two end points by stringing together multiple Access Points, where each intermediate Access Point is equipped with two radios. Because the intermediate Access Points often operate solely as relay stations, this design is referred to as Relay mode.

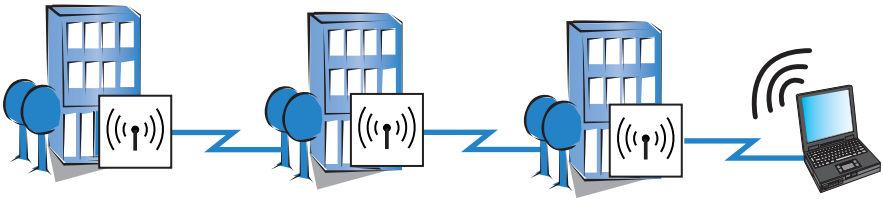


Figure 4: WLAN bridge in relay mode

OpenBAT Devices can run several P2P connections simultaneously on each wireless module, in addition to supporting WLAN Clients. However, for performance reasons, we recommend the use of OpenBAT devices with two wireless modules for the relay stations. If you use directional antennas, the relay station needs to be equipped with two radios.

1.4 WLAN Distribution Point - (Point-to-Multipoint)

A special type of wireless link is the connection of several distributed access points to a central point—the point-to-multipoint (P2MP) WLAN or Wireless Distribution System (WDS). With this mode of operation you can establish connections for several buildings on a company's premises with the central administrative building, for example. This mode of operation makes it possible, for example, for several buildings on a company's premises to be connected to the central administrative building. The central access point or wireless router is configured as 'master' and the remote stations as 'slaves'.

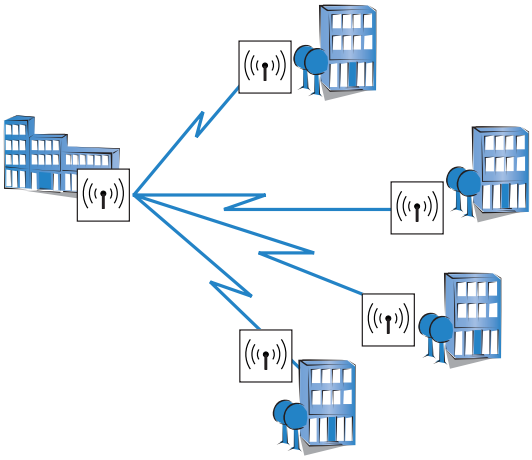


Figure 5: Point-to-multipoint wireless LAN

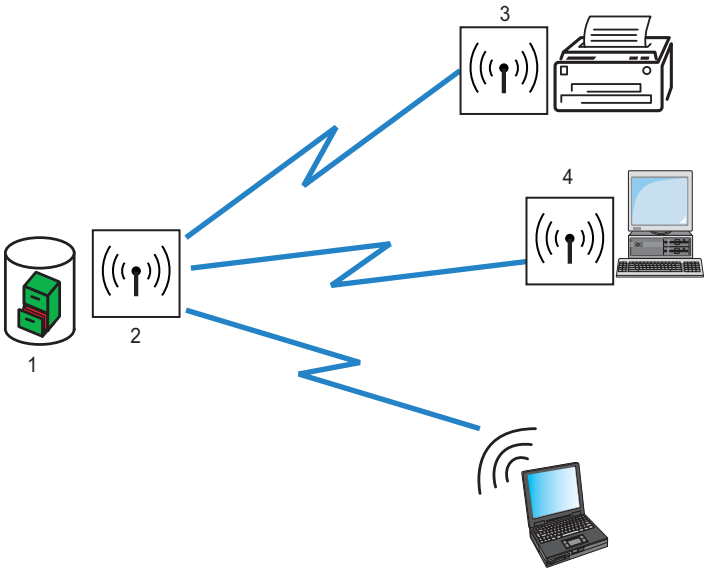
Note: A device can simultaneously establish both point-to-point and point-to-multipoint links.

1.5 WLAN Client

A WLAN Client can be either:

- equipped with an Ethernet interface (for example, a PC or printer), or
- an Access Point that is configured to serve as conventional wireless LAN adapter and not utilize its full capability as Access Point.

You can purchase special OpenBAT devices that can operate exclusively as WLAN Clients.



1: Authentication, Authorization and Accounting server	3: WLAN client with printer
2: WLAN device in Access Point mode	4: WLAN client with PC

1.6 WLAN Roaming Clients

Using OpenBAT devices, you can develop WLAN systems in industrial environments for the transmission of data to mobile objects. In the following logistics example, fork-lift trucks remain continuously connected to the company network via the WLAN. When combined with mobile barcode scanners, this system permits real-time monitoring of the inventory flow within a warehouse. Data obtained in this system pass through to an inventory control system, which continuously provides up-to-the-minute information on current inventories.

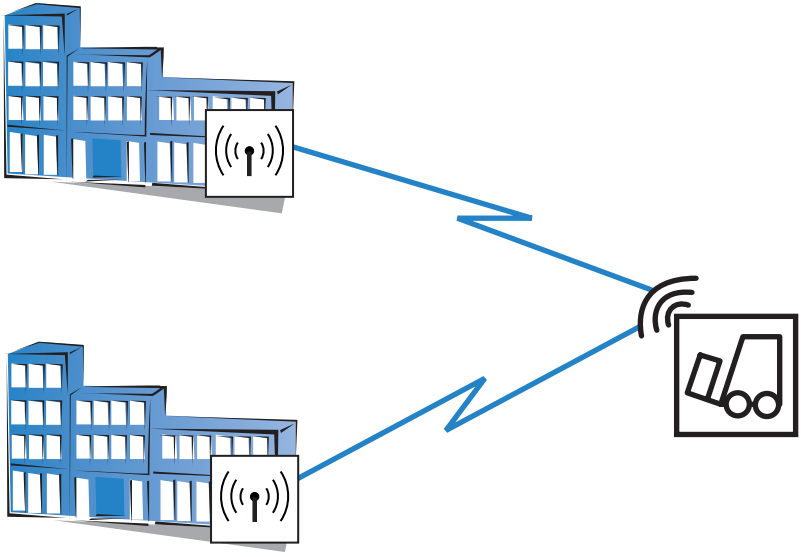


Figure 6: A WLAN client roaming between access points

2 Configuration Tools

The OpenBAT devices support a broad range of configuration software.

- LANconfig: OpenBAT device parameters can be set quickly and easily using this Windows-based application. Outband, inband and remote configurations are simultaneously supported, even for multiple devices.

- WEBconfig: This software is permanently installed in the device. All that is required on the configuration workstation is a web browser. In HiLCOS version 8.80 and above you can alternatively use the LANconfig-internal browser for accessing WEBconfig.
  WEBconfig itself works independently of the OS you run. Inband and remote configurations are supported.

- Configuring via SNMP: Device-independent applications for the management of IP networks are generally based on the SNMP protocol. The SNMP-based configuration of OpenBAT devices can be accomplished by both inband and remote access.

- Terminal program, Telnet: You can configure a OpenBAT device with a terminal program via the configuration interface (e.g. HyperTerminal) or within an IP network (e.g. Telnet).

- tftp: Trivial file transfer protocol (tftp) can also be used within IP networks (inband and remote configuration) to configure a OpenBAT device.

The following chapters of this manual present numerous configuration instructions for the OpenBAT devices. These instructions are presented using the LANconfig software.

The LANconfig menu structure for configuring an OpenBAT device:

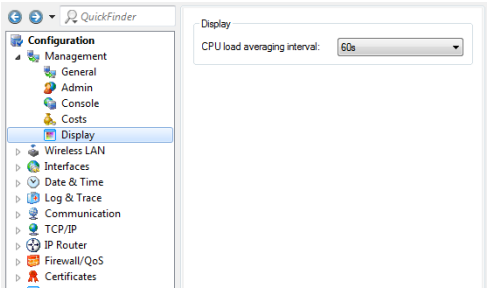
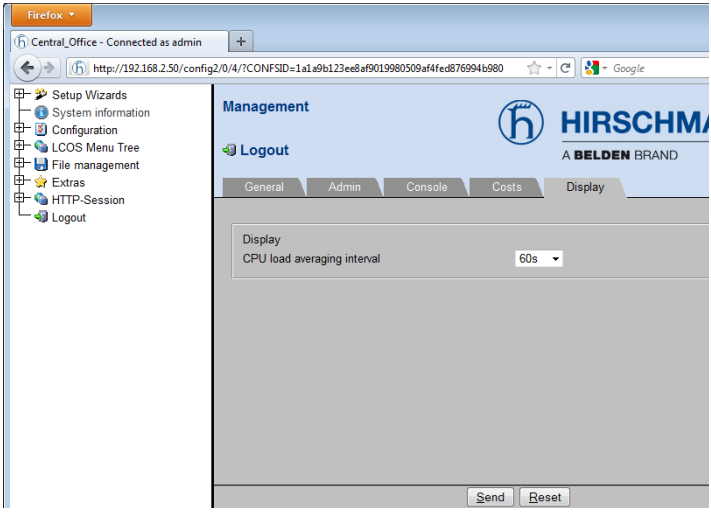


Figure 7: New Configuration of a Device

The WEBconfig menu structure for configuring an OpenBAT device:



2.1 Startup Behavior

When an OpenBAT device is shipped from the factory, it comes pre-configured with the following default settings:

- Each WLAN radio interface is turned OFF.
- The WLAN operation mode is set to ‘Managed’.

Consequently, the initial configuration of an OpenBAT device cannot be performed over the WLAN. Instead, use another means of access (e.g., via a wired LAN connection) to perform the initial configuration.

Alternatively, you can use a BAT controller to configure the Access Points conveniently from a central instance. You will find information on configuring the BAT controller under „Central WLAN Management“.

2.2 Online versus Offline Configuration

You can configure an OpenBAT device either online or offline. Each approach has its advantages:

- Online configuration is immediate—you are configuring device properties in real time.
- Offline configuration can be conducted in the controlled environment of your configuration PC. Offline configuration produces a configuration file that can be modified and re-used for similar devices.

2.3 Downloading the Configuration File

After you have created a configuration file offline, you can assign this configuration to a specific device using the LANconfig software.

☐ Use automatic discovery to 'find' the device:

  ☐ Select `File : Find devices`. The LANconfig software searches for all devices and lists the devices found.

☐ Select the device you want to configure, then go to the main menu and select: `Device : Configuration Management : Restore from file`

☐ In the 'Restore Configuration' dialog, navigate to and select the saved configuration file for the selected device, and click 'Open'.

The selected configuration file settings are applied to the device.

Note: For a more detailed description of the process of loading a configuration file to a device, see the "OpenBAT Operation and Maintenance Guide".

3 Configuring the Device

The following examples describe how you can configure OpenBAT devices in offline mode for use in the following specific applications.

- WLAN Bridge (same subnet): Two OpenBAT devices configured as Access Points, forming a point-to-point WLAN bridge connecting two segments of the same subnet
- WLAN Bridge (different subnets): Two OpenBAT devices in router mode configured as Access Points, forming a point-to-point WLAN bridge connecting two segments of different subnets
- WLAN Bridge Relay (same subnet): Two OpenBAT devices configured as Access Points, connected via a third OpenBAT device that serves as a relay device. Together, they form a point-to-point WLAN bridge.
- Point-to-Multipoint (same subnet): A single OpenBAT device configured as an Access Point for WLAN Clients, where both the wireless network and the wired network backbone are part of the same subnet
- Point-to-Multipoint (different subnets): A single OpenBAT device configured both as Access Point and as DHCP server for WLAN Clients. In this example, WLAN and wired network are located on different subnets.
- Roaming Client (different subnets): An example of a WLAN device that is configured to access a wireless LAN and obtain its IP address from a DHCP server.

In each of these examples, an OpenBAT device is configured offline, then the configuration file is downloaded to the individual device.

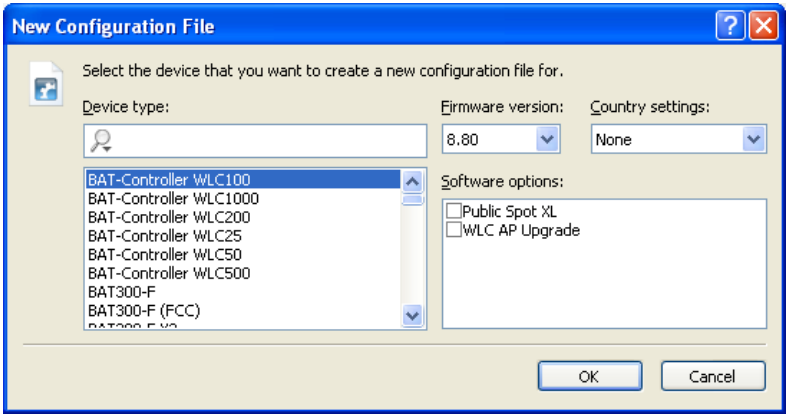
3.1 Creating a Configuration File

For all offline configurations, begin by creating a configuration file. The configuration file will contain the settings required to configure the device for service in a specific role. There are two ways to begin to create a new file:

- In the LANconfig tool's main menu, select:
  `Edit :New Configuration File`, or
- In Windows Explorer, within a folder that you have created to hold your configuration files, click the right mouse button to open a pop-up menu, then select:
  `New : Hirschmann LANconfig Configuration`

In either case, the 'New Configuration File' dialog opens. Follow the work-steps, set forth below, to create a new LANconfig file.

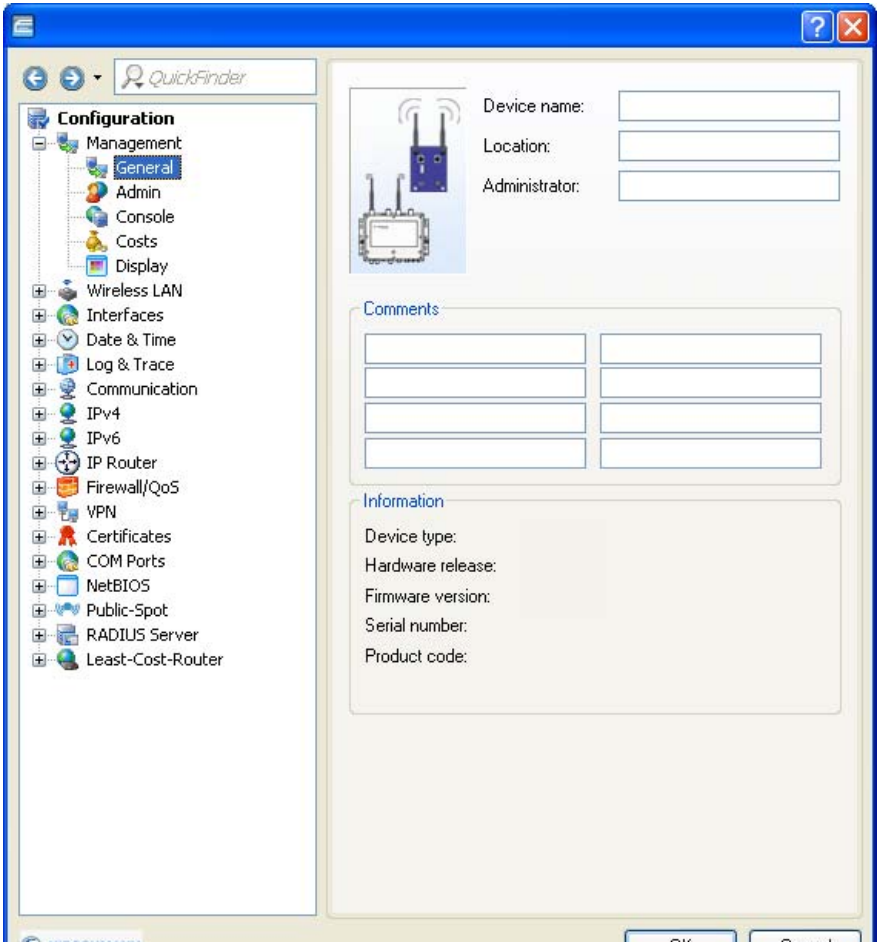
☐ In the 'New Configuration File' dialog, specify both the 'Device type' and the 'Firmware version' of the OpenBAT device you want to configure:



In this example, do the following:
- Device Type: Select a device.
- Firmware version: 8.80

– Country settings: Select a country. To ensure your device operates WLAN networks with the correct parameters, the device must be introduced to its national site. If you don't select any country settings, the device will allow only parameters that are permitted worldwide!
– Software options: Add configuration settings for additionally purchased software options to the basic configuration dialog by selecting its dedicated entry.
– Click ‘OK’.

The following dialog opens:



☐ Do the following:

☐ Type in a Device name. In this example, type in ‘LEFT’.

☐ Click ‘OK’ to save the device configuration file.

☐ Do one of the following:

– If you are working in the LANconfig tool, the ‘Save Configuration File’ dialog opens. After navigating to the desired storage location, click ‘Save’ to save the new file.

– If you are working in Windows Explorer, the ’Advanced’ dialog opens. Click ’Cancel’ to close this dialog. The new LANconfig file is saved in the Windows Explorer folder in which you are working.

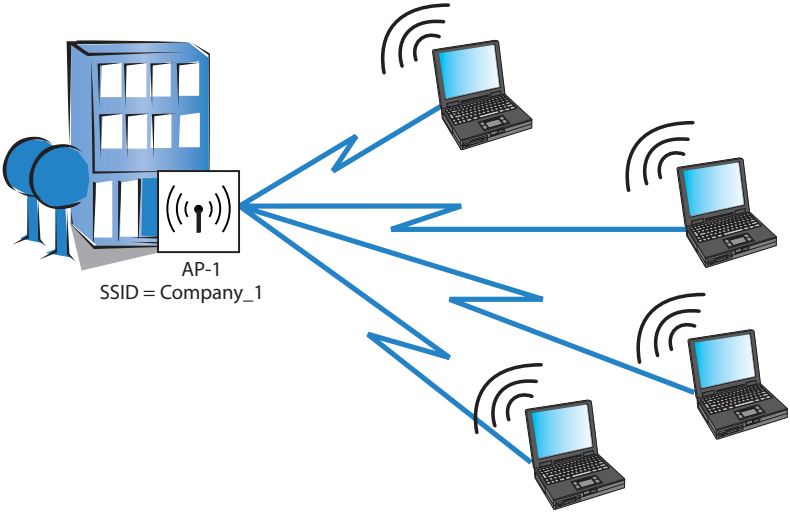
You have created and saved a new LANconfig file. The following sections describe how to configure this file for use in a specific role.

3.2 Access Point for Multiple Wireless Clients

This example describes the configuration of a single OpenBAT device (AP-1) to serve as Access Point connecting multiple WLAN Clients to a wired network. Both the wired and wireless networks are part of the same subnet. Each WLAN Client needs to select the network name (SSID) and input a pre-configured passphrase to gain access to the wireless network.

The particular IP address of any device, including both the Access Point and any WLAN Client, is not important to this design. Although the IP address for the Access Point is manually input in this example, it could instead be assigned by a DHCP server.

By deploying the completed device configuration file to multiple Access Points connected to your wired network backbone – and only changing the IP address for each Access Point – a WLAN Client could roam and stay connected to the network through a number of different Access Points.



Refer to the sample WLAN Client configuration (see on page 85) for instructions on how to set-up the clients.

The significant configuration settings for the device are as follows:

Station Name:	AP-1
Role:	Access Point
Number of interfaces/channels used:	1/1
Network name (SSID):	Company_1
WPA passphrase:	CompanyPW

Perform the following tasks to create a configuration for a OpenBAT device used in this role:

☐ Create a new configuration file

☐ Configure the basic settings

☐ Configure the wireless LAN settings

3.2.1 Creating a New Configuration File

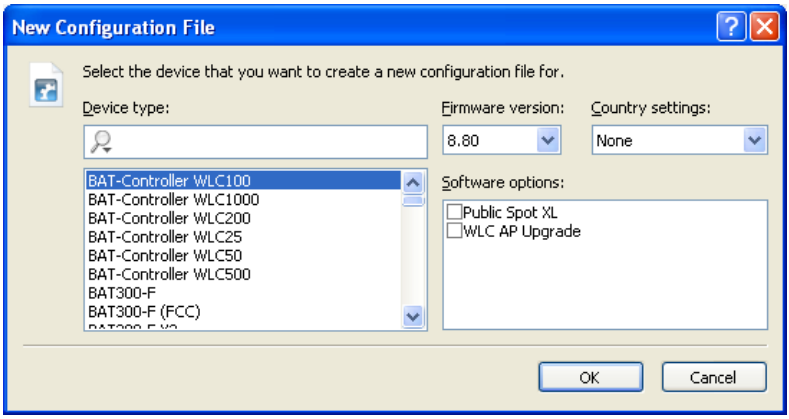
There are two ways to create a new configuration file:

☐ In the LANconfig tool's main menu, select:
`Edit :New Configuration File`, or

☐ In Windows Explorer, within a folder that you have created to hold your configuration files, click the right mouse button to open a pop-up menu, then select:
`New : Hirschmann LANconfig Configuration`

In either case, the ‘New Configuration File’ dialog opens. Follow the work-steps, set forth below, to create a new LANconfig file.

☐ In the ‘New Configuration File’ dialog, specify both the ‘Device type’ and the ‘Firmware version’ of the OpenBAT device you want to configure:

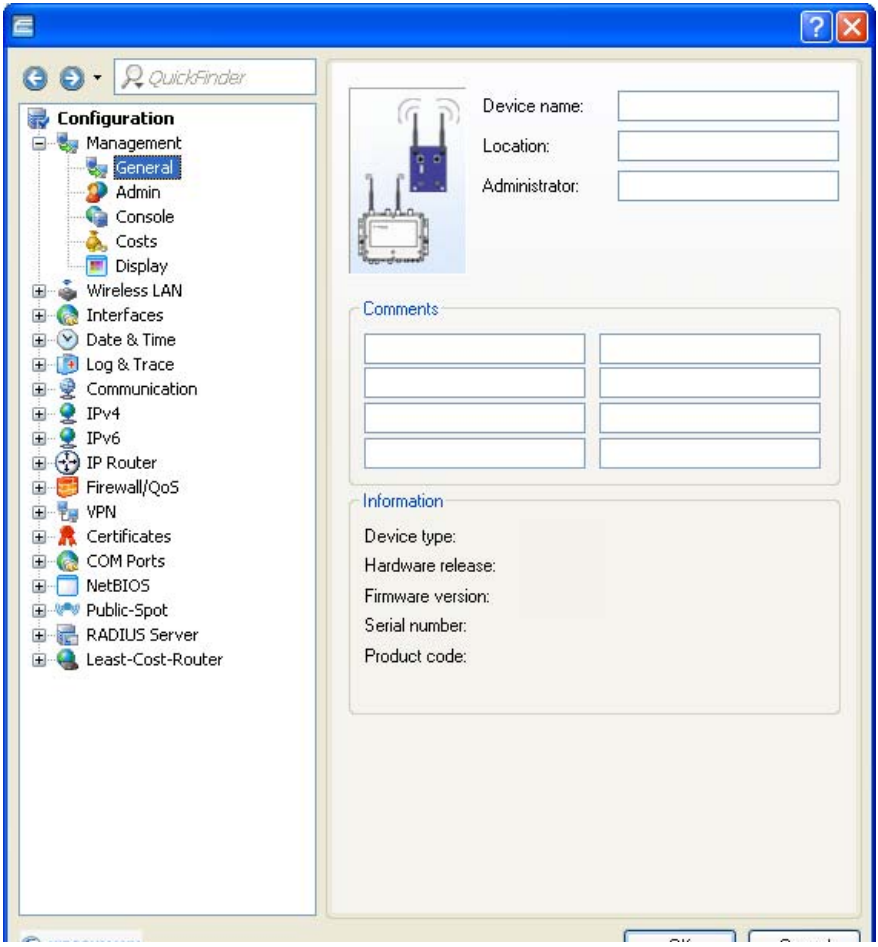


In this example, do the following:

– Device Type: Select a device.
– Firmware version: 8.80
– Country settings: Select a country. To ensure your device operates WLAN networks with the correct parameters, the device must be introduced to its national site. If you don't select any country settings, the device will allow only parameters that are permitted worldwide!

– Software options: Add configuration settings for additionally purchased software options to the basic configuration dialog by selecting its dedicated entry.
– Click ‘OK’.

The following dialog opens:



☐ Do the following:

  ☐ Type in a Device name. In this example, type in 'AP-1'.

  ☐ Click 'OK' to save the device configuration file.

☐ Do one of the following:

  – If you are working in the LANconfig tool, the 'Save Configuration File' dialog opens. After navigating to the desired storage location, click 'Save' to save the new file.

  – If you are working in Windows Explorer, the 'Advanced' dialog opens. Click 'Cancel' to close this dialog. The new LANconfig file is saved in the Windows Explorer folder in which you are working.

☐ Open Windows Explorer, navigate to the new file, and change its name to `AP-1.lcf`.

You have created and saved a new LANconfig file. The following sections describe how to configure this file for use as a wireless access point.

3.2.2 Configuring Basic Settings

Use the LANconfig Setup Wizard to configure the following basic settings for the device configuration file:

– device name

– password

– DHCP mode

– TCP/IP settings

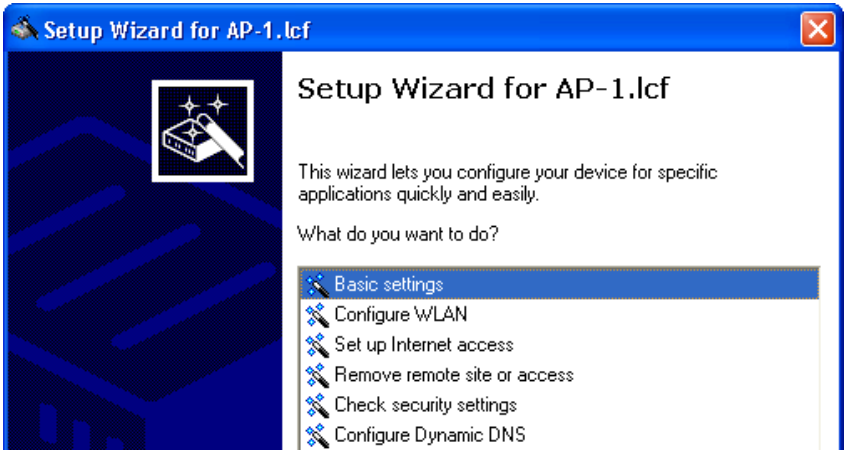
– time synchronization settings
– optional device descriptions

☐ To start the Setup Wizard:

☐ In Windows Explorer, select the newly created LANconfig file, then

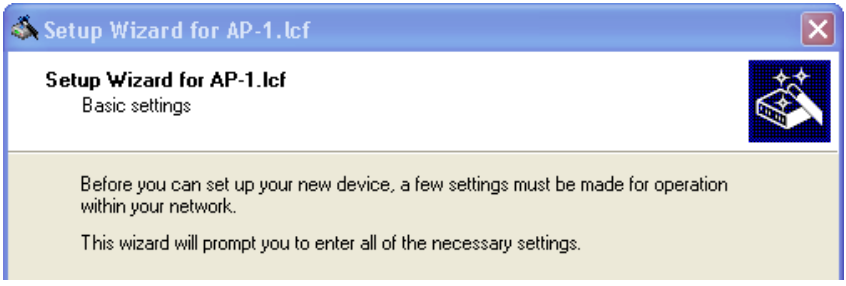
☐ Click the right mouse button to open a pop-up menu, then select `Setup Wizard`.

☐ In the Setup Wizard, select 'Basic settings':


Setup Wizard for AP-1.lcf
Setup Wizard for AP-1.lcf
This wizard lets you configure your device for specific applications quickly and easily.
What do you want to do?
Basic settings
Configure WLAN
Set up Internet access
Remove remote site or access
Check security settings
Configure Dynamic DNS

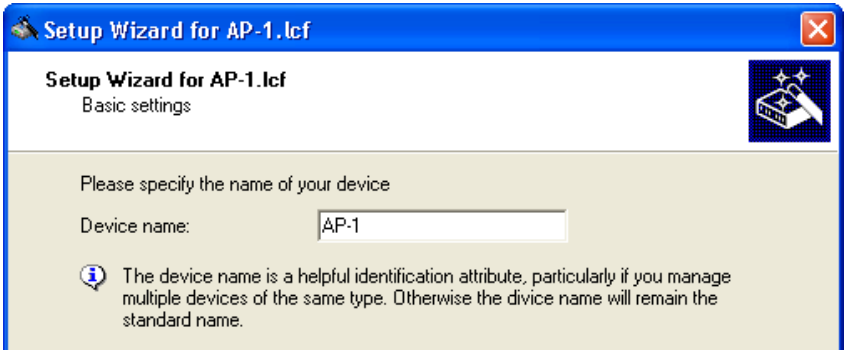
Click 'Next'.

☐ The wizard displays the following introduction:


Setup Wizard for AP-1.lcf
Setup Wizard for AP-1.lcf
Basic settings
Before you can set up your new device, a few settings must be made for operation within your network.
This wizard will prompt you to enter all of the necessary settings.

Click ’Next’.

☐ Input a device name:


Setup Wizard for AP-1.lcf
Setup Wizard for AP-1.lcf
Basic settings
Please specify the name of your device
Device name:
AP-1
The device name is a helpful identification attribute, particularly if you manage multiple devices of the same type. Otherwise the divice name will remain the standard name.

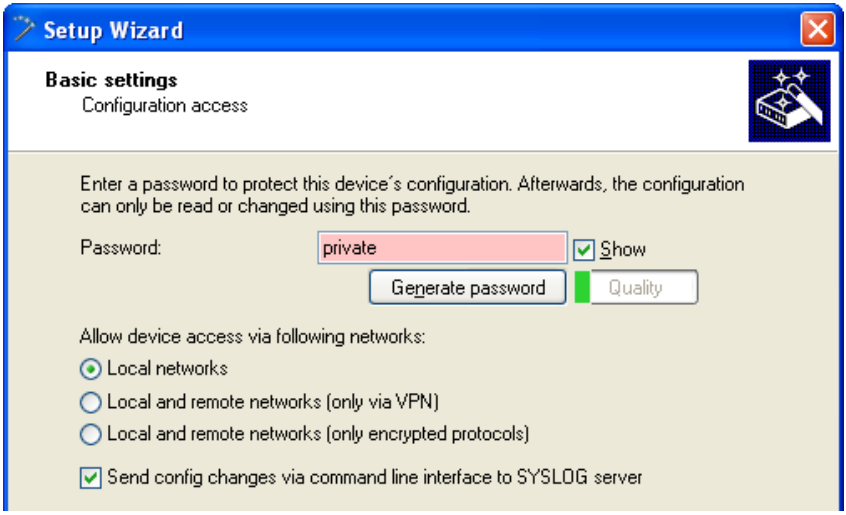
For the purpose of this example, use the name ’AP-1’.

Note: The default device name is a concatenation of the device part number and the last 3 octets of the device MAC address.

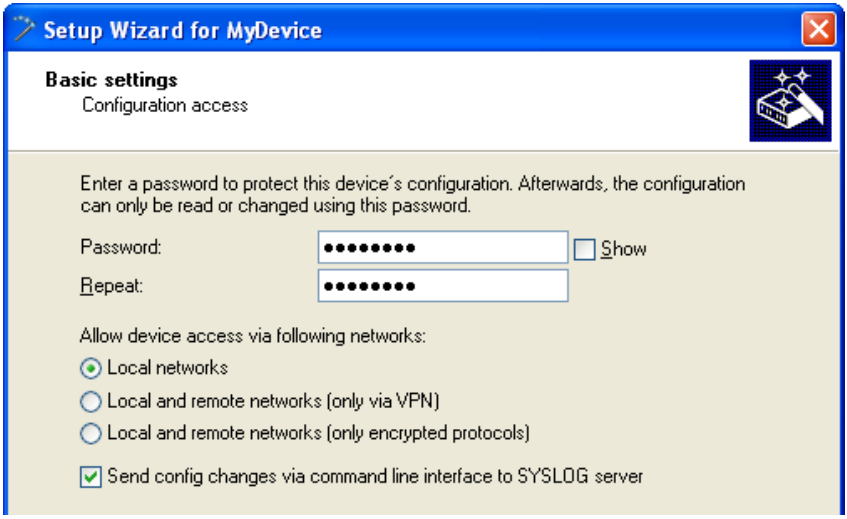
Click ’Next’.

☐ The following screen opens, where you need to enter a password in one of the following ways:

- Select 'Show' (below) to display the default password ('private') then do one of the following:
  - accept the default password
  - type in a new password
  - click 'Generate password' to let the wizard input a new password


Setup Wizard
Basic settings
Configuration access
Enter a password to protect this device´s configuration. Afterwards, the configuration can only be read or changed using this password.
Password:
private
Show
Generate password
Quality
Allow device access via following networks:
Local networks
Local and remote networks (only via VPN)
Local and remote networks (only encrypted protocols)
Send config changes via command line interface to SYSLOG server

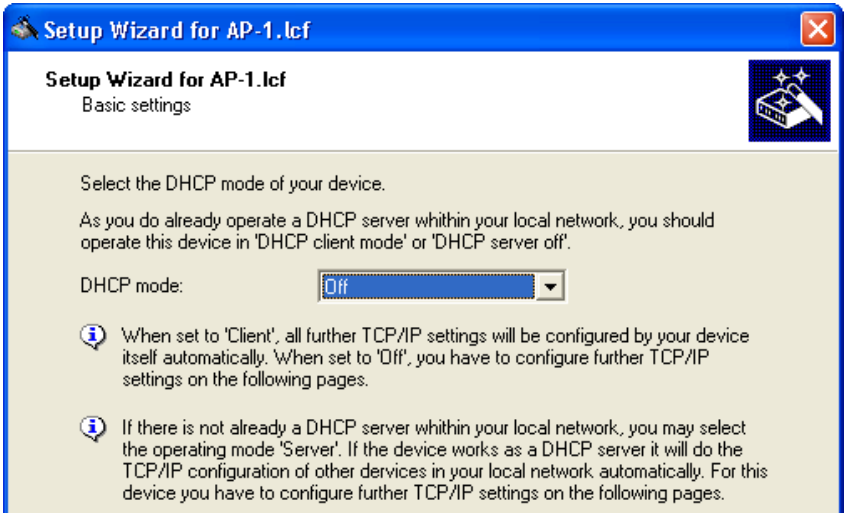
- De-select 'Show' (below) then either accept the default password ('private') or type in a new one. In either case, re-type the password in the 'Repeat' field.


Setup Wizard for MyDevice
Basic settings
Configuration access
Enter a password to protect this device´s configuration. Afterwards, the configuration can only be read or changed using this password.
Password:
Show
Repeat:
Allow device access via following networks:
Local networks
Local and remote networks (only via VPN)
Local and remote networks (only encrypted protocols)
Send config changes via command line interface to SYSLOG server

▶ Set the networks permitted to access the device. If you restrict access to local networks, only PCs that are directly connected to the local area network by cable or wireless can access the device configuration.

Note: The assistent indicates the different security levels of passwords color-coded. Insecure passwords are highlighted in red, conditionally secure ones are highlighted in yellow, and secure to very secure ones are highlighted in white.

☐ Identify the DHCP mode of the OpenBAT device:


Setup Wizard for AP-1.lcf
Setup Wizard for AP-1.lcf
Basic settings
Select the DHCP mode of your device.
As you do already operate a DHCP server whithin your local network, you should operate this device in 'DHCP client mode' or 'DHCP server off'.
DHCP mode:
Off
When set to 'Client', all further TCP/IP settings will be configured by your device itself automatically. When set to 'Off', you have to configure further TCP/IP settings on the following pages.
If there is not already a DHCP server whithin your local network, you may select the operating mode 'Server'. If the device works as a DHCP server it will do the TCP/IP configuration of other dervices in your local network automatically. For this device you have to configure further TCP/IP settings on the following pages.

Select one of the following DHCP modes:

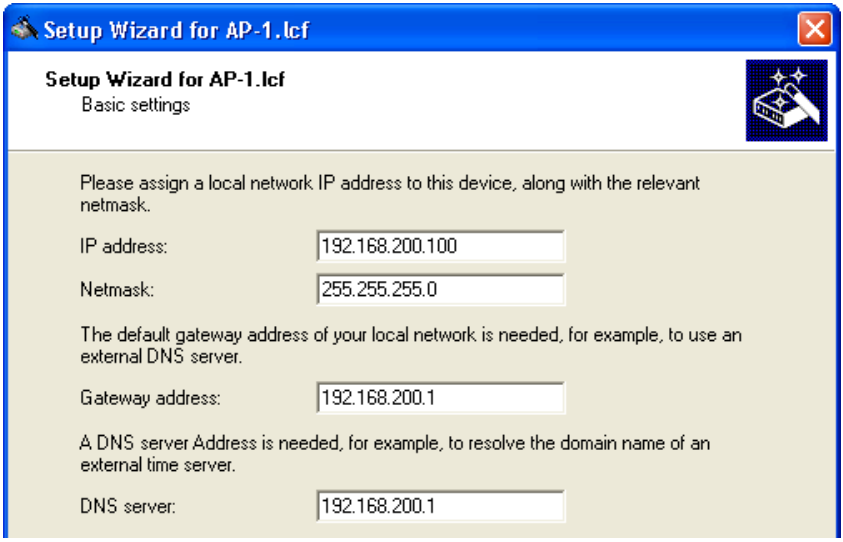
– Off:
  The device functions neither as DHCP client nor as DHCP server. In this mode, you need to manually input the IP address settings.
– Server:
  The OpenBAT device functions as DHCP server and provides IP address settings to other network devices.
– Client:
  This setting causes the OpenBAT device to request the IP address settings from a DHCP server on the network.

If a DHCP server exists on your network, select the ‘DHCP mode’ of ‘Off’. The default ‘DHCP mode’ setting of ‘Client’ can override a manually assigned IP address.

Note: Your DHCP mode selection determines the next screen displayed by the Setup Wizard.

For the purpose of this example, select ’Off’, then click ’Next’.

☐ Input the TCP/IP settings for the OpenBAT device:

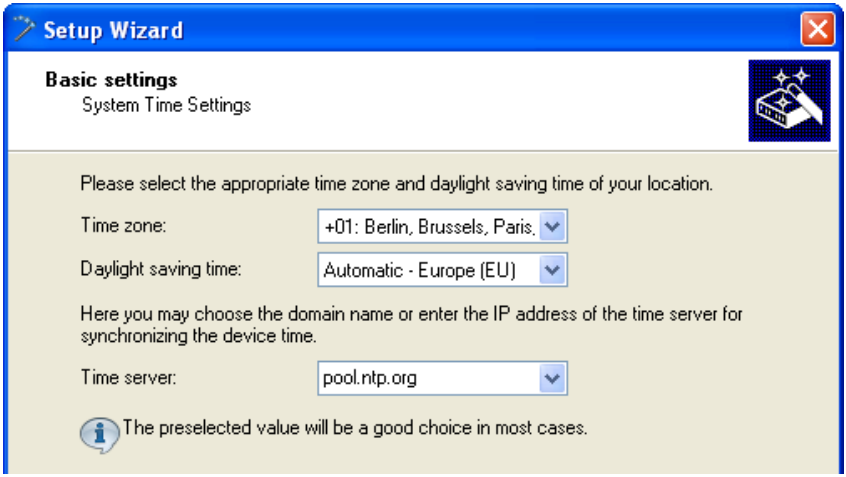

Setup Wizard for AP-1.lcf
Setup Wizard for AP-1.lcf
Basic settings
Please assign a local network IP address to this device, along with the relevant netmask.
IP address:
192.168.200.100
Netmask:
255.255.255.0
The default gateway address of your local network is needed, for example, to use an external DNS server.
Gateway address:
192.168.200.1
A DNS server Address is needed, for example, to resolve the domain name of an external time server.
DNS server:
192.168.200.1

For the purpose of this example, these settings are:

- IP address: 192.168.200.100
- Netmask: 255.255.255.0
- Gateway address: 192.168.200.1
- DNS server: 192.168.200.1

Click 'Next'.

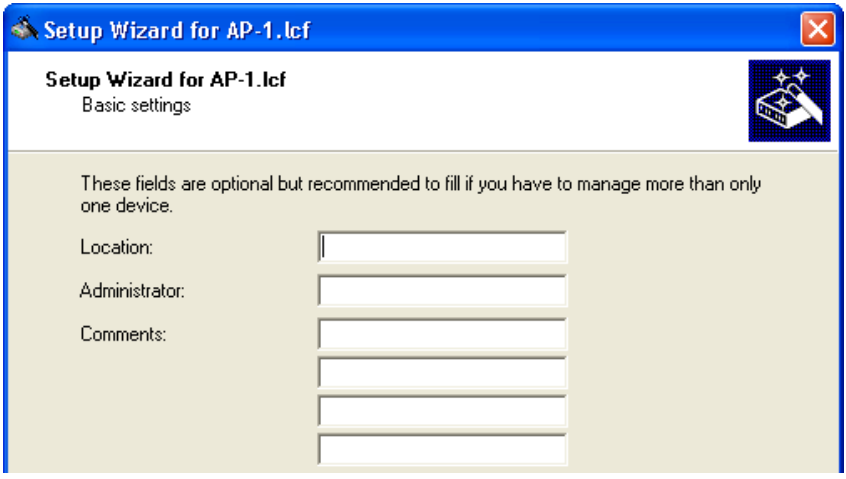
☐ The wizard prompts you to identify your national timezone, prevailing changeover rules and a time synchronization server that will set the system time for the OpenBAT device:


Setup Wizard
Basic settings
System Time Settings
Please select the appropriate time zone and daylight saving time of your location.
Time zone:
+01: Berlin, Brussels, Paris.
Daylight saving time:
Automatic - Europe (EU)
Here you may choose the domain name or enter the IP address of the time server for synchronizing the device time.
Time server:
pool.ntp.org
The preselected value will be a good choice in most cases.

Select a time server from the list, or type in its IP address.

Click 'Next'.

☐ The wizard shows the following screen for optional information on the location of the device, its administrator, and any comments relating to the OpenBAT device.


Setup Wizard for AP-1.lcf
Setup Wizard for AP-1.lcf
Basic settings
These fields are optional but recommended to fill if you have to manage more than only one device.
Location:
Administrator:
Comments:

Click 'Next'.

☐ Click 'Finish' to complete configuration of the basic settings (below):

Setup Wizard for AP-1.lcf
Setup Wizard for AP-1.lcf
You have configured all necessary basic settings required for a proper device startup.
Please select 'Finish' to apply the new settings.
The process may take about 60 seconds. After that the setup wizard restarts and further settings may be done.

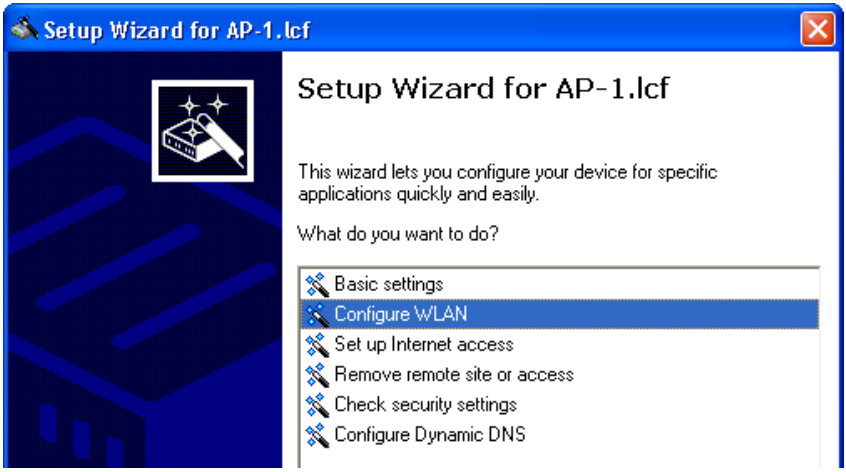
3.2.3 Configuring Wireless LAN Settings

WLAN settings can be made using either the LANconfig tool's discrete configuration screens or the Setup Wizard. This task is most easily accomplished using the wizard.

☐ To start the Setup Wizard:

- ☐ In Windows Explorer, select the current LANconfig file, then
- ☐ Click the right mouse button to open a pop-up menu, then select `Setup Wizard`.

☐ In the wizard, select 'Configure WLAN' (below):


Setup Wizard for AP-1.lcf
Setup Wizard for AP-1.lcf
This wizard lets you configure your device for specific applications quickly and easily.
What do you want to do?
Basic settings
Configure WLAN
Set up Internet access
Remove remote site or access
Check security settings
Configure Dynamic DNS

Click 'Next'.

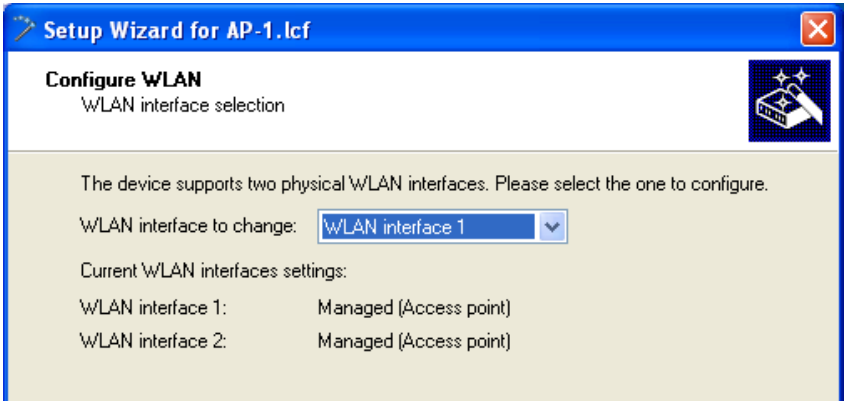
☐ Select the country in which the OpenBAT device is operated:

Setup Wizard for AP-1.lcf
Configure WLAN
Edit physical WLAN settings
The device must know its country location in order to use the correct wireless base settings.
Please select the country in which the device will be operated.
Country:
USA

Note: The country designation determines the available frequencies.

Click 'Next'.

☐ Select a WLAN interface to configure:

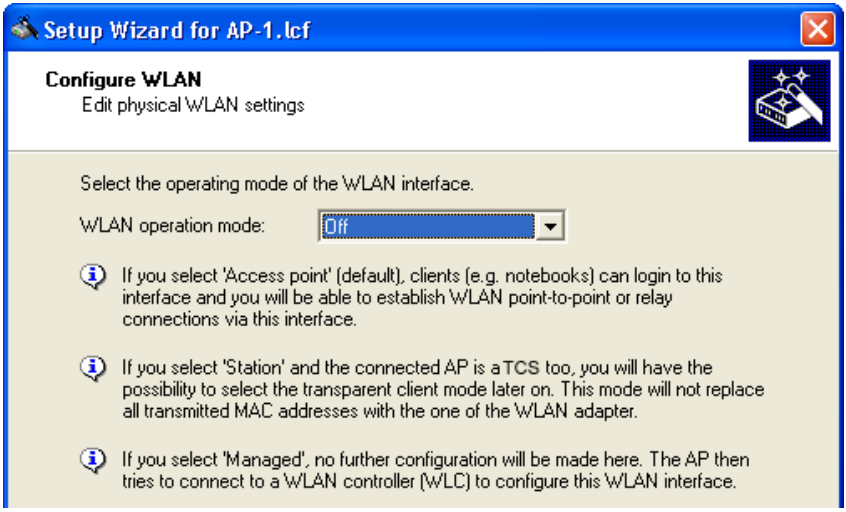

Setup Wizard for AP-1.lcf
Configure WLAN
WLAN interface selection
The device supports two physical WLAN interfaces. Please select the one to configure.
WLAN interface to change:
WLAN interface 1
Current WLAN interfaces settings:
WLAN interface 1: Managed (Access point)
WLAN interface 2: Managed (Access point)

A device can have multiple WLAN interfaces. Here, the selected device has two (2) interfaces. By default, both interfaces are enabled.

Note: You can configure one WLAN interface at a time. After selecting an interface, proceed through the wizard's remaining pages and finish configuration for the selected interface. Thereafter, re-start the Configure WLAN wizard and configure the other WLAN interface.

Select 'WLAN interface 2' as the WLAN interface to configure (above), then click 'Next'.

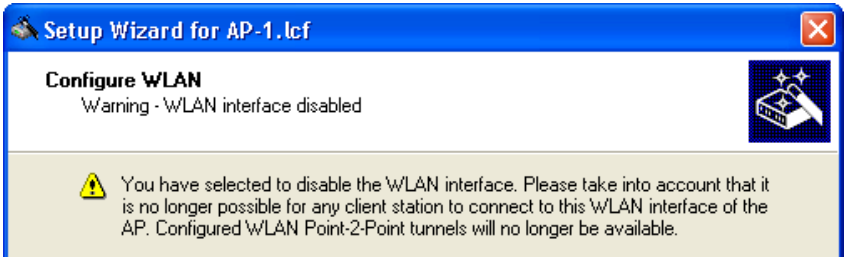
☐ The next step is to enable or disable the selected WLAN interface:


Setup Wizard for AP-1.lcf
Configure WLAN
Edit physical WLAN settings
Select the operating mode of the WLAN interface.
WLAN operation mode:
Off
If you select 'Access point' (default), clients (e.g. notebooks) can login to this interface and you will be able to establish WLAN point-to-point or relay connections via this interface.
If you select 'Station' and the connected AP is a TCS too, you will have the possibility to select the transparent client mode later on. This mode will not replace all transmitted MAC addresses with the one of the WLAN adapter.
If you select 'Managed', no further configuration will be made here. The AP then tries to connect to a WLAN controller (WLC) to configure this WLAN interface.

A point-to-point WLAN bridge requires just a single interface. In this example, the currently selected interface—WLAN interface 2—will be disabled. (You will later configure WLAN interface 1 to support the point-to-point WLAN bridge.)

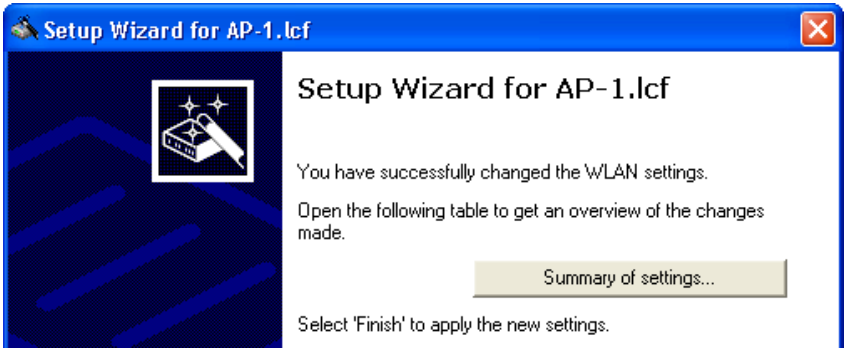
Disable WLAN interface 2 by setting its ’WLAN operation mode’ to ’Off’ (above), then click ‘Next’.

☐ The wizard notifies you that you are about to disable interface 2:


Setup Wizard for AP-1.lcf
Configure WLAN
Warning - WLAN interface disabled
You have selected to disable the WLAN interface. Please take into account that it is no longer possible for any client station to connect to this WLAN interface of the AP. Configured WLAN Point-2-Point tunnels will no longer be available.

Click ’Next’.

☐ Complete the configuration of WLAN interface 2:


Setup Wizard for AP-1.lcf
Setup Wizard for AP-1.lcf
You have successfully changed the WLAN settings.
Open the following table to get an overview of the changes made.
Summary of settings...
Select 'Finish' to apply the new settings.

Click ’Finish’.

☐ Return to the Windows Explorer folder where the file LANconfig file is saved, then do the following:

– select the LANconfig file (`AP-1.lcf`)

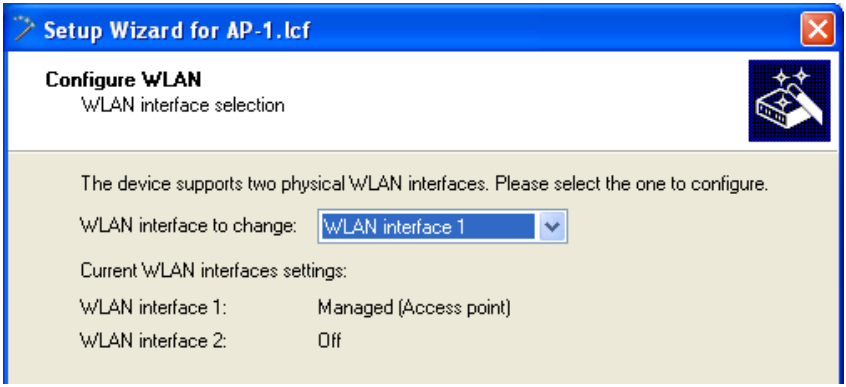
– click the right mouse button to open a pop-up menu

– select `Setup Wizard`

☐ In the LANconfig Setup Wizard:

☐ select ’Configure WLAN’

☐ click ’Next’ two times, or until the wizard displays the WLAN interface selection screen

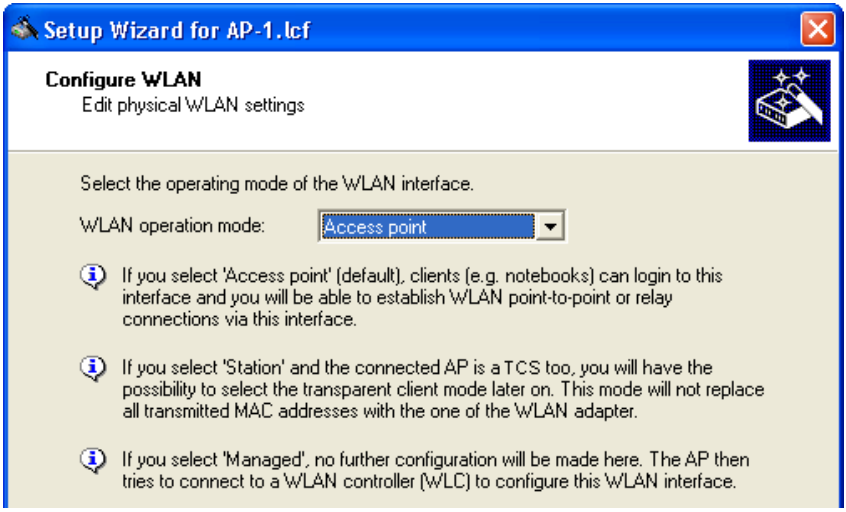

Setup Wizard for AP-1.lcf
Configure WLAN
WLAN interface selection
The device supports two physical WLAN interfaces. Please select the one to configure.
WLAN interface to change:
WLAN interface 1
Current WLAN interfaces settings:
WLAN interface 1: Managed (Access point)
WLAN interface 2: Off

Note: This screen indicates that WLAN interface 2 has been turned off. The next step is to configure WLAN interface 1.

Select 'WLAN interface 1' as the 'WLAN interface to change'.

Click 'Next'.

☐ Specify an operation mode for the interface (WLAN interface 1):


Setup Wizard for AP-1.lcf
Configure WLAN
Edit physical WLAN settings
Select the operating mode of the WLAN interface.
WLAN operation mode:
Access point
If you select 'Access point' (default), clients (e.g. notebooks) can login to this interface and you will be able to establish WLAN point-to-point or relay connections via this interface.
If you select 'Station' and the connected AP is a TCS too, you will have the possibility to select the transparent client mode later on. This mode will not replace all transmitted MAC addresses with the one of the WLAN adapter.
If you select 'Managed', no further configuration will be made here. The AP then tries to connect to a WLAN controller (WLC) to configure this WLAN interface.

WLAN operation modes include:

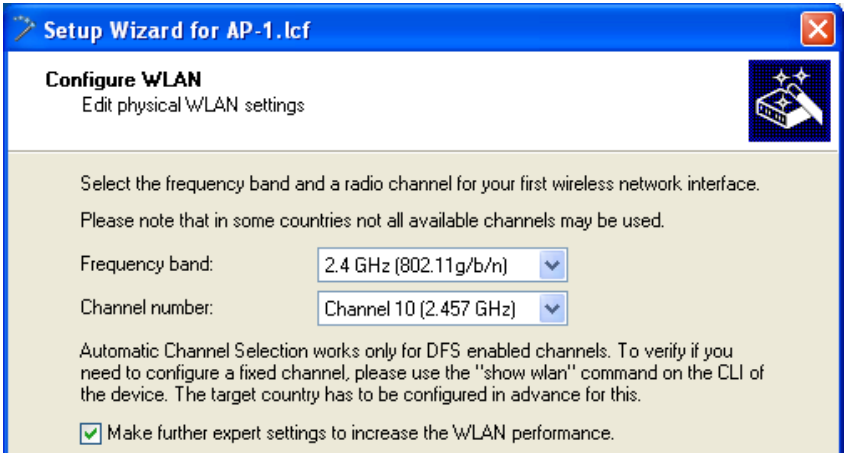
– Access Point:
The device serves as a base station, and can establish links to another access point (point-to-point), to remote clients, or to both remote access points and remote clients.

– Client:
The device serves as Client and needs to log into an Access Point. In this role, the device can link a cabled network to a WLAN over a wireless connection.

– Managed (Access point):
The device operates as an Access point, but searches for a central WLAN controller it can obtain a configuration from.

Select ’Access point’, then click ’Next’.

☐ Enter settings for the wireless frequency and channels over which the device will operate, and indicate whether you wish to configure additional performance-enhancing settings:


Setup Wizard for AP-1.lcf
Configure WLAN
Edit physical WLAN settings
Select the frequency band and a radio channel for your first wireless network interface.
Please note that in some countries not all available channels may be used.
Frequency band:
2.4 GHz (802.11g/b/n)
Channel number:
Channel 10 (2.457 GHz)
Automatic Channel Selection works only for DFS enabled channels. To verify if you need to configure a fixed channel, please use the "show wlan" command on the CLI of the device. The target country has to be configured in advance for this.
Make further expert settings to increase the WLAN performance.

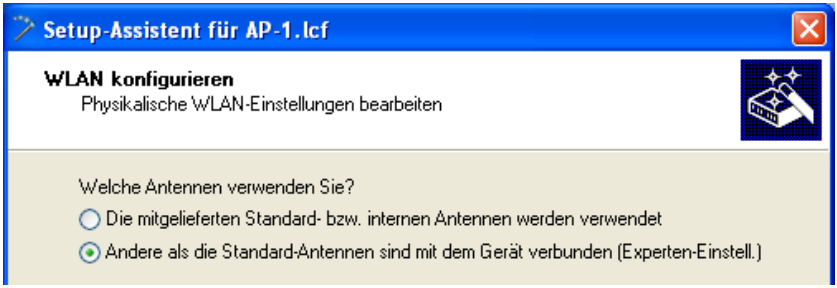
The specific antennas you plan to use will determine how you complete this dialog. For the purpose of this example, enter the following settings:

– Frequency band: 2.4 GHz

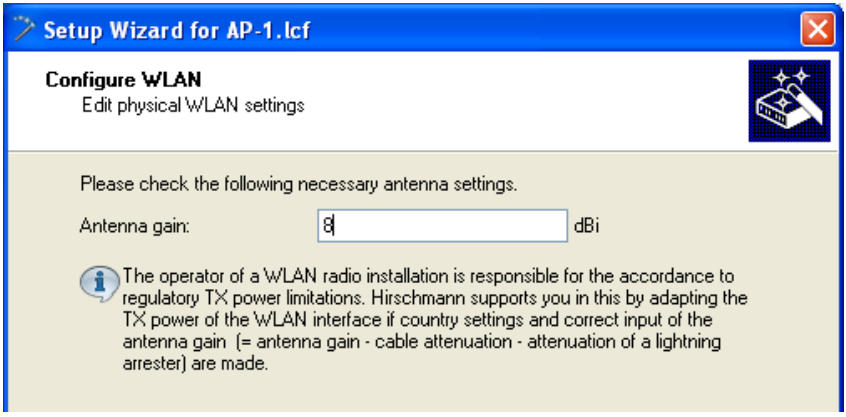
– Channel number: Channel 10 (2.457 GHz)

– Select ‘Make further explicit settings to increase the WLAN performance’.
(This option gets the set-up wizard to display additional configuration screens for QoS and IGMP snooping.)

– Choose: ‘Antennas other than the default antennas are connected to the device.’

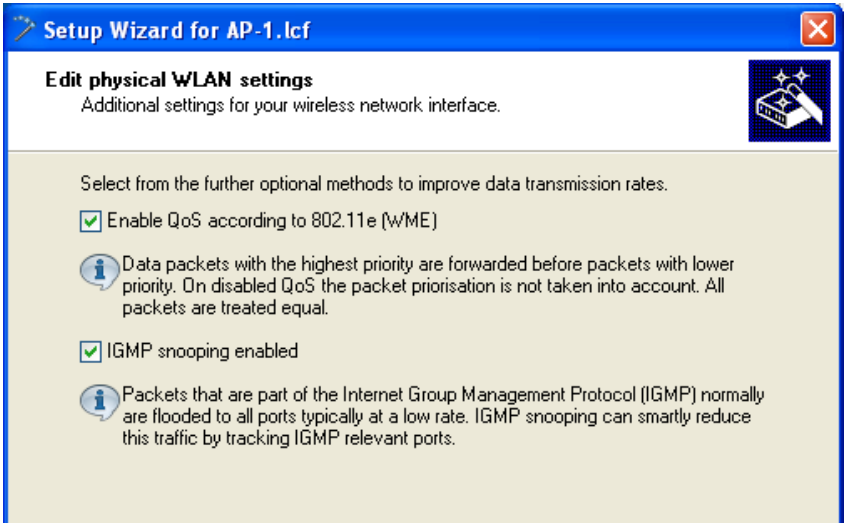

Setup-Assistent für AP-1.lcf
WLAN konfigurieren
Physikalische WLAN-Einstellungen bearbeiten
Welche Antennen verwenden Sie?
Die mitgelieferten Standard- bzw. internen Antennen werden verwendet
Andere als die Standard-Antennen sind mit dem Gerät verbunden (Experten-Einstell.)

☐ Check the antenna settings:


Setup Wizard for AP-1.lcf
Configure WLAN
Edit physical WLAN settings
Please check the following necessary antenna settings.
Antenna gain:
8
dBi
The operator of a WLAN radio installation is responsible for the accordance to regulatory TX power limitations. Hirschmann supports you in this by adapting the TX power of the WLAN interface if country settings and correct input of the antenna gain (= antenna gain - cable attenuation - attenuation of a lightning arrester) are made.

the calculated antenna gain is 8 dBi for this example

☐ Click 'Next'.
The wizard presents settings that can be used to increase data transmission rates:


Setup Wizard for AP-1.lcf
Edit physical WLAN settings
Additional settings for your wireless network interface.
Select from the further optional methods to improve data transmission rates.
Enable QoS according to 802.11e (WME)
Data packets with the highest priority are forwarded before packets with lower priority. On disabled QoS the packet priorisation is not taken into account. All packets are treated equal.
IGMP snooping enabled
Packets that are part of the Internet Group Management Protocol (IGMP) normally are flooded to all ports typically at a low rate. IGMP snooping can smartly reduce this traffic by tracking IGMP relevant ports.

You can enable or disable the following services:

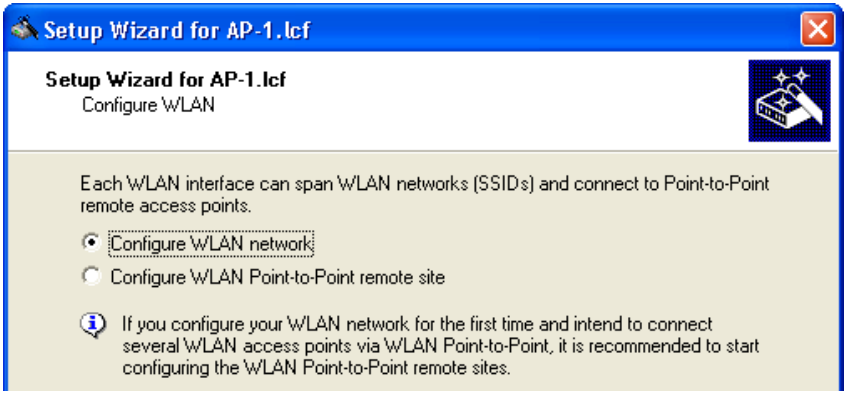
– QoS

– IGMP Snooping

For the purpose of this example, all available data rate enhancing options are selected.

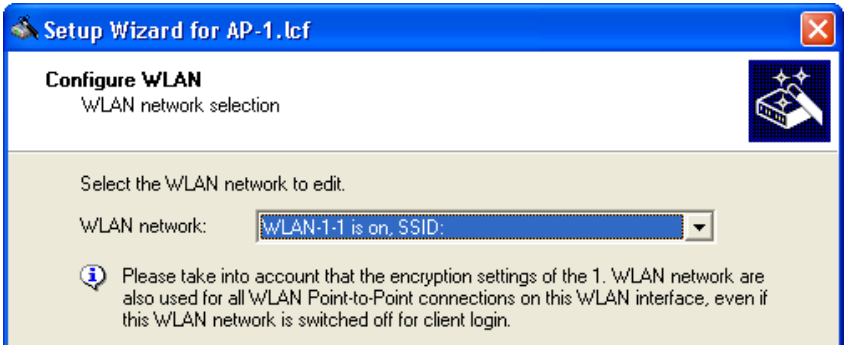
Click ’Next’.

☐ Indicate what will be configured—a point-to-point site or a WLAN network:


Setup Wizard for AP-1.lcf
Setup Wizard for AP-1.lcf
Configure WLAN
Each WLAN interface can span WLAN networks (SSIDs) and connect to Point-to-Point remote access points.
Configure WLAN network
Configure WLAN Point-to-Point remote site
If you configure your WLAN network for the first time and intend to connect several WLAN access points via WLAN Point-to-Point, it is recommended to start configuring the WLAN Point-to-Point remote sites.

Select 'Configure WLAN network', then click 'Next'.

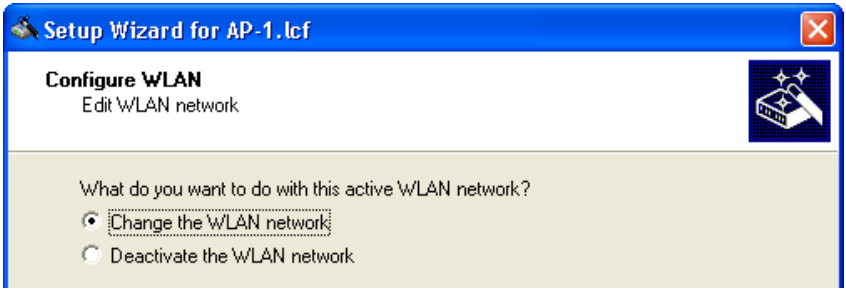
☐ Select the network to configure:


Setup Wizard for AP-1.lcf
Configure WLAN
WLAN network selection
Select the WLAN network to edit.
WLAN network:
WLAN-1-1 is on, SSID:
Please take into account that the encryption settings of the 1. WLAN network are also used for all WLAN Point-to-Point connections on this WLAN interface, even if this WLAN network is switched off for client login.

For the WLAN network, select 'WLAN-1-1'. This indicates that this access point will use channel 1 on interface 1.

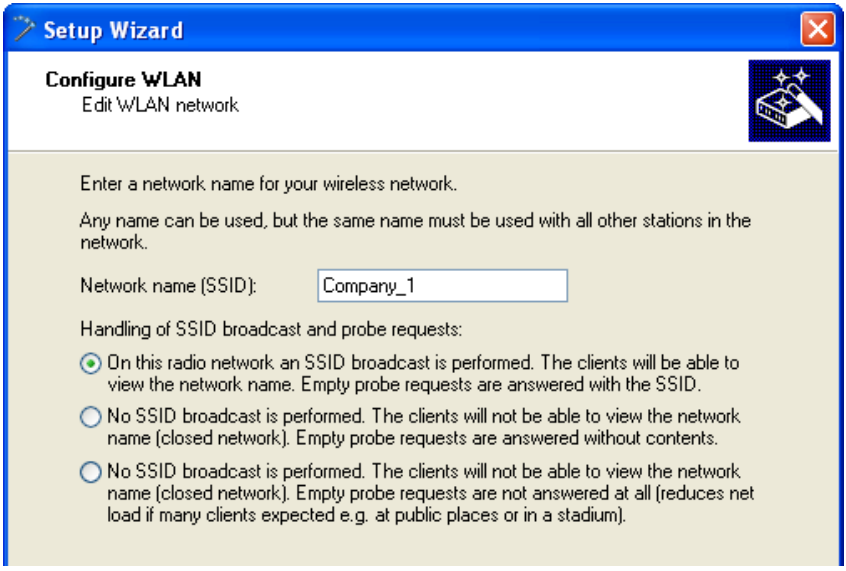
Click 'Next'.

☐ Indicate that changes are to be made to the WLAN network:


Setup Wizard for AP-1.lcf
Configure WLAN
Edit WLAN network
What do you want to do with this active WLAN network?
Change the WLAN network
Deactivate the WLAN network

Select 'Change the WLAN network, then click 'Next'.

☐ Enter the Network name (also known as the Service Set Identifier or 'SSID'):


Setup Wizard
Configure WLAN
Edit WLAN network
Enter a network name for your wireless network.
Any name can be used, but the same name must be used with all other stations in the network.
Network name (SSID):
Company_1
Handling of SSID broadcast and probe requests:
On this radio network an SSID broadcast is performed. The clients will be able to view the network name. Empty probe requests are answered with the SSID.
No SSID broadcast is performed. The clients will not be able to view the network name (closed network). Empty probe requests are answered without contents.
No SSID broadcast is performed. The clients will not be able to view the network name (closed network). Empty probe requests are not answered at all (reduces net load if many clients expected e.g. at public places or in a stadium).

Also, select whether the device should propagate the specified SSID in its wireless network. If you disable the SSID broadcast, the device does not transmit any SSID. This can help keep rogue wireless client devices from detecting the existence of this network.

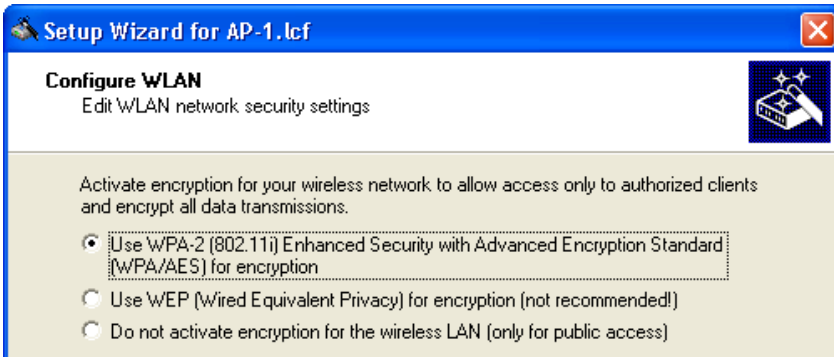
For the purpose of this example:

– Change the SSID to ’Company_1’

– Option "No SSID broadcast is performed […]".

Click ’Next’.

☐ Specify the transmission encryption protocol:

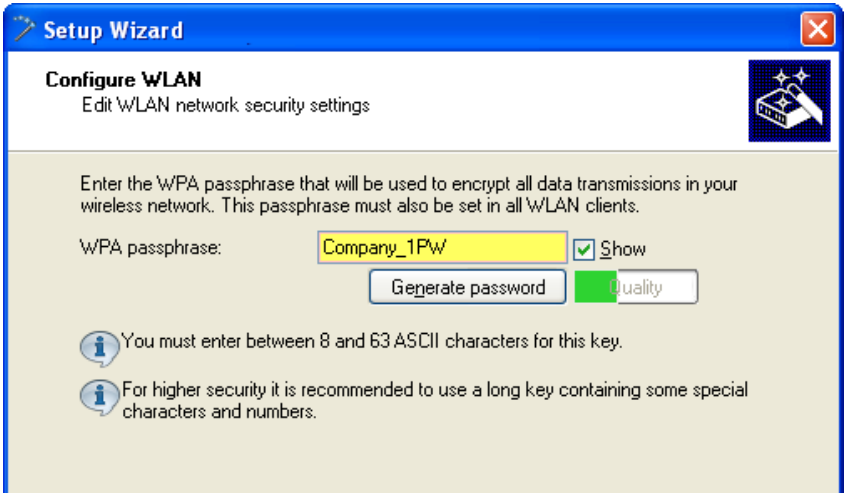

Setup Wizard for AP-1.lcf
Configure WLAN
Edit WLAN network security settings
Activate encryption for your wireless network to allow access only to authorized clients and encrypt all data transmissions.
Use WPA-2 (802.11i) Enhanced Security with Advanced Encryption Standard (WPA/AES) for encryption
Use WEP (Wired Equivalent Privacy) for encryption (not recommended!)
Do not activate encryption for the wireless LAN (only for public access)

Note: Hirschmann recommends the use of WPA-2 to provide enhanced security.

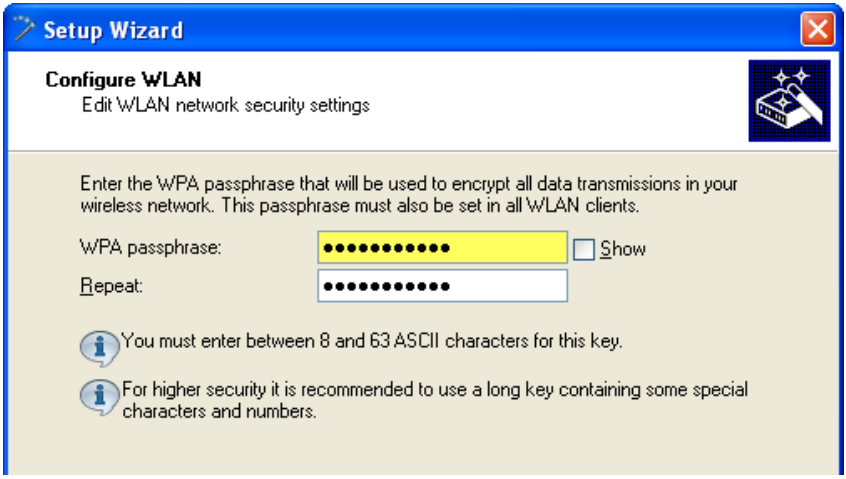
Click ’Next’.

☐ The following screen opens, where you enter a password in one of the following ways:

– Select 'Show' (below) to enter a WPA passphrase then either:
  - type in a new passphrase
  - click 'Generate password' to let the wizard input a new passphrase


Setup Wizard
Configure WLAN
Edit WLAN network security settings
Enter the WPA passphrase that will be used to encrypt all data transmissions in your wireless network. This passphrase must also be set in all WLAN clients.
WPA passphrase:
Company_1PW
Show
Generate password
Quality
You must enter between 8 and 63 ASCII characters for this key.
For higher security it is recommended to use a long key containing some special characters and numbers.

– deactivate the 'Show' checkbox (below) and enter a new WPA passphrase. For this you use a key with 8 to 63 ASCII characters, using special characters and numbers if possible. Then repeat the entry in the 'Repeat' field.


Setup Wizard
Configure WLAN
Edit WLAN network security settings
Enter the WPA passphrase that will be used to encrypt all data transmissions in your wireless network. This passphrase must also be set in all WLAN clients.
WPA passphrase:
Show
Repeat:
You must enter between 8 and 63 ASCII characters for this key.
For higher security it is recommended to use a long key containing some special characters and numbers.

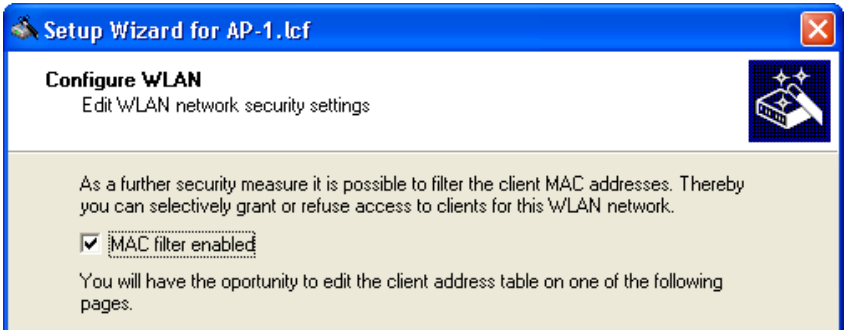
The role of an OpenBAT device in the point-to-point connection determines how the passphrase is used. If the device is configured as:

– Master: the passphrase is used to check a slave's authorization to access the network.

– Slave: the passphrase is transferred to the Master to gain wireless access to the network.

In this example, accept the default password, then click 'Next'.

☐ Indicate whether the MAC filter will be used by this WLAN:


Setup Wizard for AP-1.lcf
Configure WLAN
Edit WLAN network security settings
As a further security measure it is possible to filter the client MAC addresses. Thereby you can selectively grant or refuse access to clients for this WLAN network.
MAC filter enabled
You will have the oportunity to edit the client address table on one of the following pages.

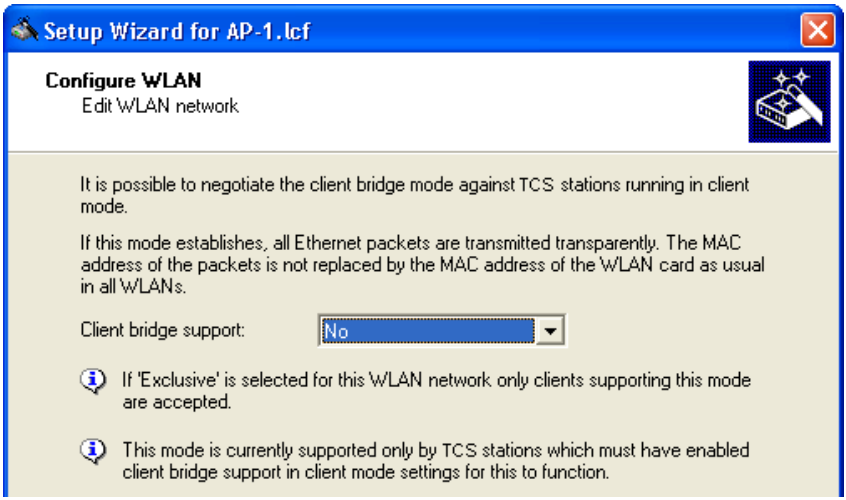
The OpenBAT device can filter WLAN Client devices based on a list of MAC addresses. The list can be either a:

- blacklist, denying network access to listed MAC addresses, or
- whitelist, limiting network access exclusively to listed MAC addresses

Select the 'MAC filter enabled' checkbox. Later, the MAC filter will be configured for use as a blacklist.

Click 'Next'.

☐ Indicate whether client bridge support will be enabled:


Setup Wizard for AP-1.lcf
Configure WLAN
Edit WLAN network
It is possible to negotiate the client bridge mode against TCS stations running in client mode.
If this mode establishes, all Ethernet packets are transmitted transparently. The MAC address of the packets is not replaced by the MAC address of the WLAN card as usual in all WLANs.
Client bridge support:
No
If 'Exclusive' is selected for this WLAN network only clients supporting this mode are accepted.
This mode is currently supported only by TCS stations which must have enabled client bridge support in client mode settings for this to function.

Client bridge support relates to a network design that consists of:

– an OpenBAT device in the role of Access Point
– an OpenBAT device in the role of client
– one or more remote Ethernet devices connected to the client OpenBAT device in client mode

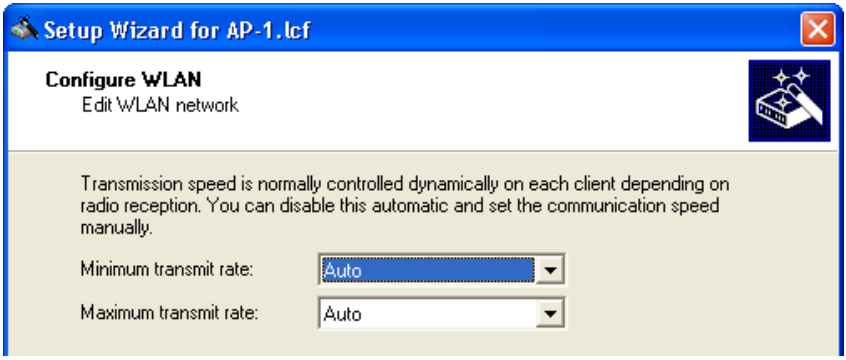
Typically, packets sent from a remote Ethernet device to the access point via the wireless client contain the MAC address of the wireless client, exclusively. Enabling client bridge support also includes the MAC address of the remote device.

Client bridging options are:

– No: client bridging support by the access point is disabled
– Yes: client bridging support by the access point is enabled
– Exclusive: wireless clients with enabled client bridging can communicate with the access point

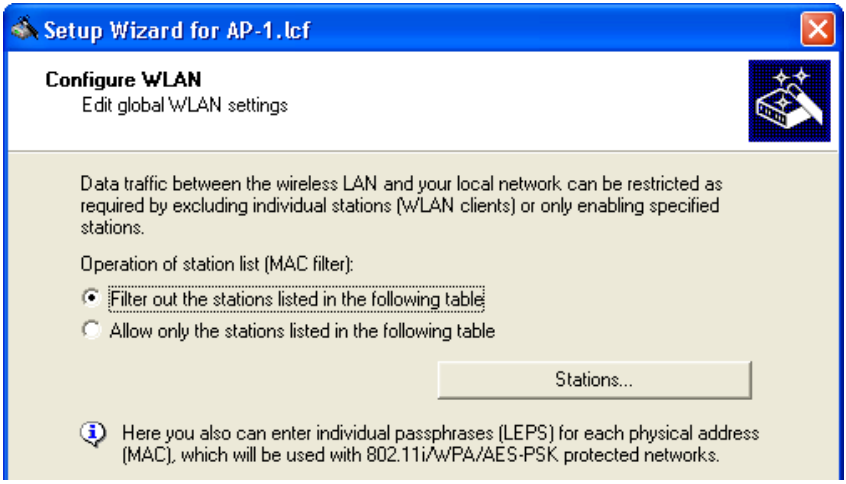
For this example, select ’No’ to disable client bridging, then click ’Next’.

☐ Specify how transmission speed between the access point and wireless clients will be determined:


Setup Wizard for AP-1.lcf
Configure WLAN
Edit WLAN network
Transmission speed is normally controlled dynamically on each client depending on radio reception. You can disable this automatic and set the communication speed manually.
Minimum transmit rate:
Auto
Maximum transmit rate:
Auto

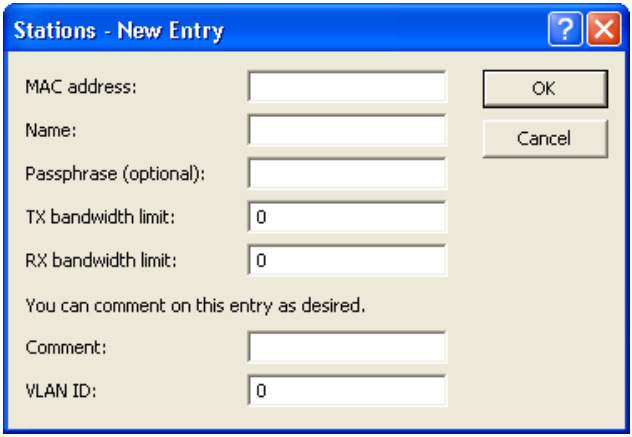
Select ’Auto’ for both the ‘Minimum transmit rate’ and the ‘Maximum transmit rate’, then click ’Next’.

☐ Enter settings for the MAC filter:


Setup Wizard for AP-1.lcf
Configure WLAN
Edit global WLAN settings
Data traffic between the wireless LAN and your local network can be restricted as required by excluding individual stations (WLAN clients) or only enabling specified stations.
Operation of station list (MAC filter):
Filter out the stations listed in the following table
Allow only the stations listed in the following table
Stations...
Here you also can enter individual passphrases (LEPS) for each physical address (MAC), which will be used with 802.11i/WPA/AES-PSK protected networks.

☐ Select 'Filter out the stations listed in the following table' (above), then click the 'Stations...' button to open the following table:

☐ Click 'Add...' (above) to open the 'New Entry' dialog (below):

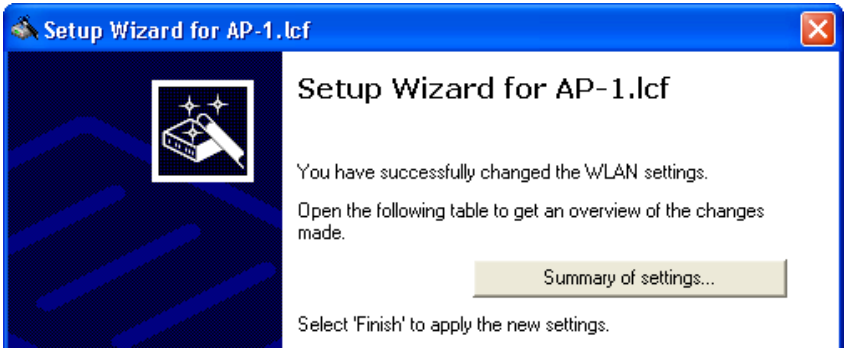


Use the' New Entry' dialog to add individual wireless client stations that will be denied access to the network. The lone parameter that needs to be configured for access denial is 'MAC address'.

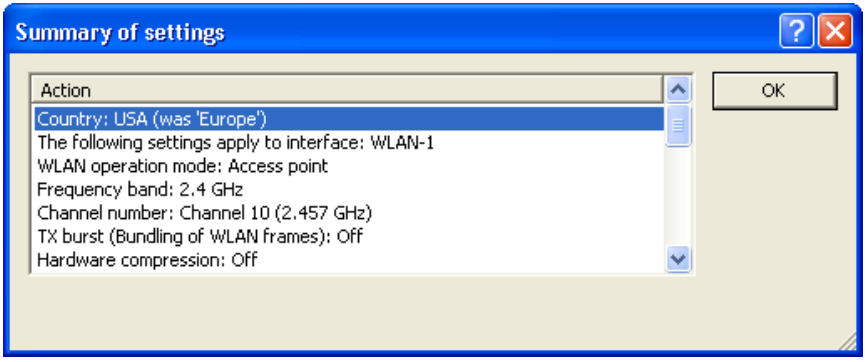
Note: When creating a 'whitelist', you can use:
- the Passphrase field to assign a device-specific passphrase
- the Bandwidth fields to restrict transmissions to a specific bandwidth
- the VLAN ID field to assign a client device to a VLAN

Click 'OK' to add a station. After all stations are added (one at a time), click 'OK' to close the list and return to the Configure WLAN wizard.

☐ You are now ready to complete the configuration of the access point for the wireless network:


Setup Wizard for AP-1.lcf
Setup Wizard for AP-1.lcf
You have successfully changed the WLAN settings.
Open the following table to get an overview of the changes made.
Summary of settings...
Select 'Finish' to apply the new settings.

☐ Click on the ’Summary of settings...’ button to display a list of all WLAN configuration settings:


Summary of settings
Action
Country: USA (was 'Europe')
The following settings apply to interface: WLAN-1
WLAN operation mode: Access point
Frequency band: 2.4 GHz
Channel number: Channel 10 (2.457 GHz)
TX burst (Bundling of WLAN frames): Off
Hardware compression: Off
OK

Click ’OK’ to close the ‘Summary of settings’ window.

Click ’Finish’ to complete the wizard and save the settings for this wireless network access point.

3.3 Access Point & DHCP Server for Multiple Wireless Clients

This example builds on the previous configuration of an Access Point for multiple WLAN clients (see on page 47), by configuring the OpenBAT device (in this example, AP-2) to perform the additional role of DHCP server. In this example, the wired and wireless networks are located on different subnets. As before, each WLAN Client needs to select the network name (SSID) and input a pre-configured passphrase to gain access to the wireless network.

When a WLAN Client initially accesses the wireless network, the Access Point - in its role as DHCP server - dynamically assigns the client an IP address. Because the WLAN Clients are located on their own subnet, WLAN Clients are not able to transmit broadcasts or other unwanted data traffic that might flood the wired network backbone.

The tasks to be performed in this configuration example include:

- Create a new configuration file (`AP-2.lcf`) by copying the previously created file (`AP-1.lcf`).
- Edit the existing 'INTRANET' IP network to serve exclusively as wired LAN.
- Create and configure a new DHCP network to serve exclusively as wireless LAN.

3.3.1 Creating a New Configuration File

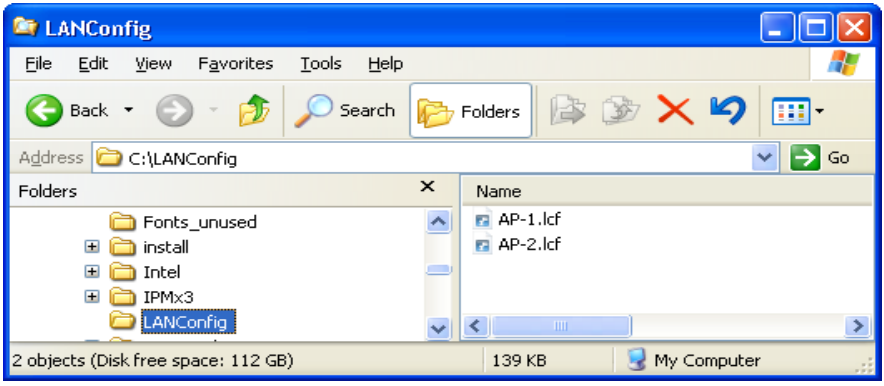
To create a new LANconfig configuration file, follow these steps:

☐ In Windows Explorer, navigate to the folder where the file `AP-1.lcf` is located and copy it.

☐ Paste the copied file into your choice of folder in Windows Explorer.

☐ Rename the new file `AP-2.lcf`.

If you copied the new file into the same folder as the old one, Windows Explorer contains the following files:

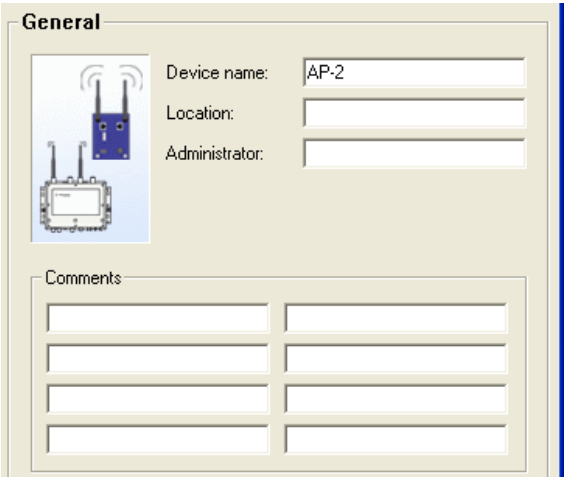


3.3.2 Changing the Existing Network to a Wired LAN

Configure the existing INTRANET IP network to serve exclusively as a wired LAN:

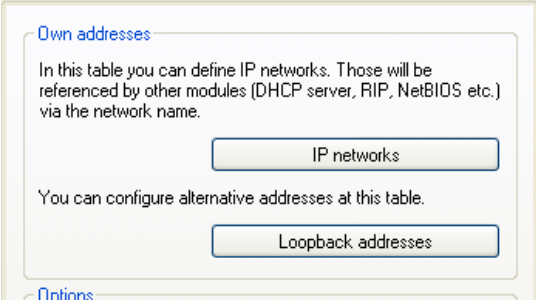
☐ In Windows Explorer, double-click the file `AP-2.lcf` to open it for editing.

☐ Open the `Configuration : Management : General` dialog:

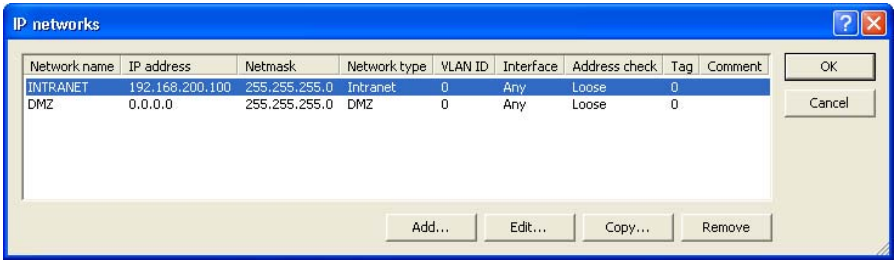


Change the Device name to 'AP-2'.

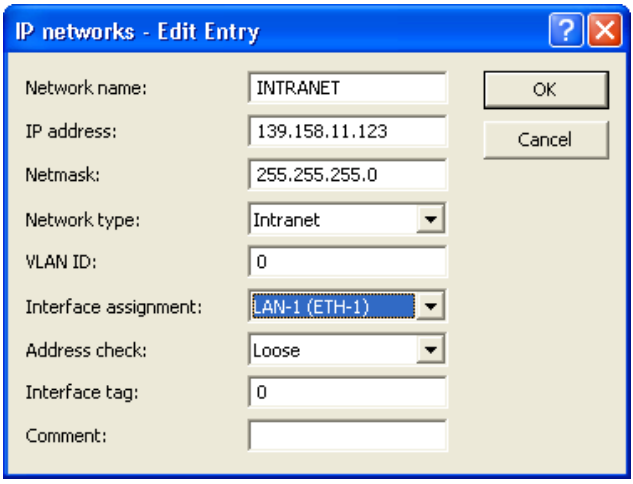
☐ Open the `Configuration : IPv4 : General`.


Own addresses
In this table you can define IP networks. Those will be referenced by other modules (DHCP server, RIP, NetBIOS etc.) via the network name.
IP networks
You can configure alternative addresses at this table.
Loopback addresses
Options

Click the 'IP networks' button (above) to open the 'IP networks' window (below):



☐ Select the 'INTRANET' network in the list, then click on 'Edit...' to open the 'Edit Entry' dialog, below:

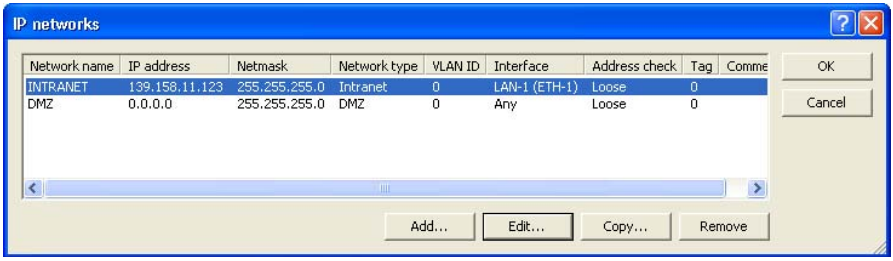


Convert the existing INTRANET network to a wired Ethernet LAN by editing the following settings:

– IP address: 139.158.11.123

– Interface assignment: LAN-1 (ETH-1)

Click 'OK' to close the 'Edit Entry' dialog and return to the 'IP networks' window, below:



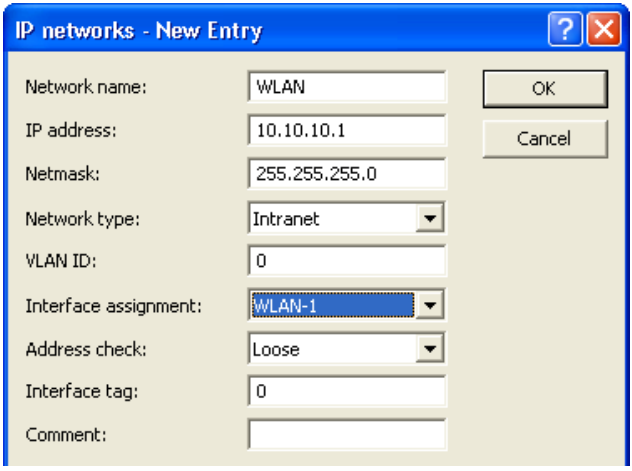
Leave the ‘IP networks’ window open.

3.3.3 Create a New DHCP Wireless LAN

Next, create a new DHCP network to be used exclusively as a Wireless LAN:

☐ In the ‘IP networks’ window, click ’Add...’ to open the ‘New Entry’ dialog.

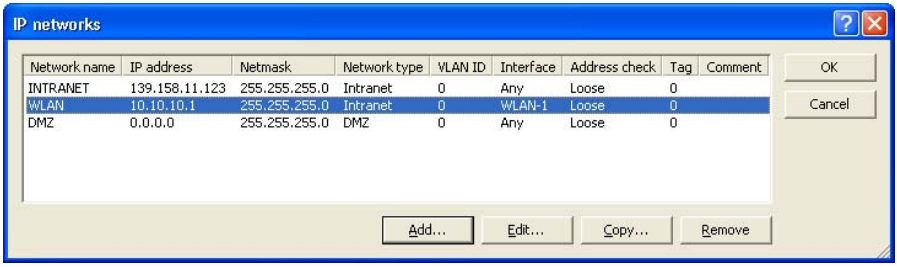
☐ In the ‘New Entry’ dialog, below, create a new wireless LAN network:



Enter the following settings for the new wireless LAN network:

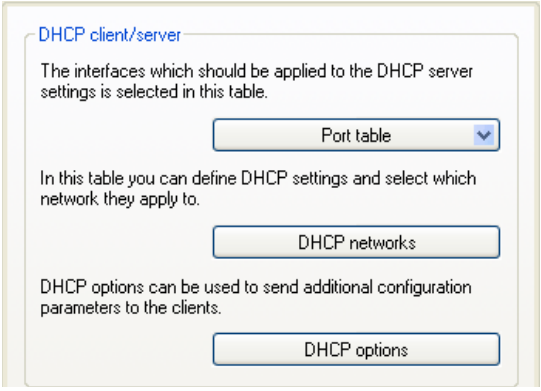
– Network name: 'WLAN'
– IP address: '10.10.10.1'
– Network type: 'Intranet'
– Interface assignment: 'WLAN-1'

Click 'OK' to close the 'New Entry' dialog and add the new wireless LAN network to the IP network list (below):

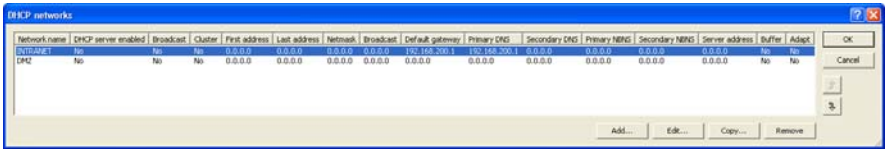


Click 'OK' again to close the 'IP networks' window (above).

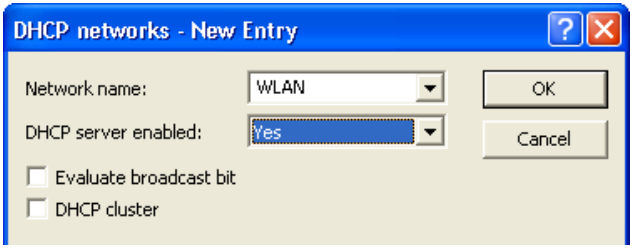
☐ The DHCP server is enabled inside the `Configuration : IPv4 : DHCPv4` dialog.


DHCP client/server
The interfaces which should be applied to the DHCP server settings is selected in this table.
Port table
In this table you can define DHCP settings and select which network they apply to.
DHCP networks
DHCP options can be used to send additional configuration parameters to the clients.
DHCP options

Click the 'DHCP networks...' button (above) to open the 'DHCP networks' window (below):



☐ In the ‘DHCP networks’ window (above), click ’Add...’ to open the ‘New Entry’ dialog (below):

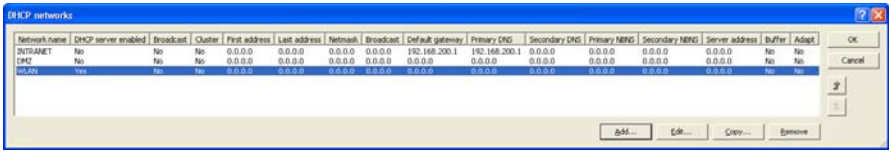


Edit the following fields by making the following selections:

– Network name: ’WLAN’

– DHCP server enabled: ’Yes’

Click ’OK’ to close the ‘New Entry’ dialog.
A new DHCP network appears in the DHCP networks window, below:



☐ Click ’OK’ to close the DHCP networks window.

Click ’OK’ again to close the LANconfig file and save your edits.

The `AP-2.lcf` file is configured for use as both a Wireless access point and a DHCP server.

3.4 Wireless Client

This example shows you how to configure a OpenBAT device that is designed exclusively for the role of WLAN Client. The most significant settings to be configured are the:

– SSID or name of the wireless network to which the Client will be connected, and

– DHCP mode (in this case DHCP client), indicating the source of the device's IP address settings

The following tasks are described in this example:

- Create a new LANconfig file
- Configure basis settings for the client device
- Configure WLAN settings for the client device

3.4.1 Creating a New LANconfig File for a Client

Follow these steps to create a new client LANconfig file:

In either case, the 'New Configuration File' dialog opens. Follow the work-steps, set forth below, to create a new LANconfig file.

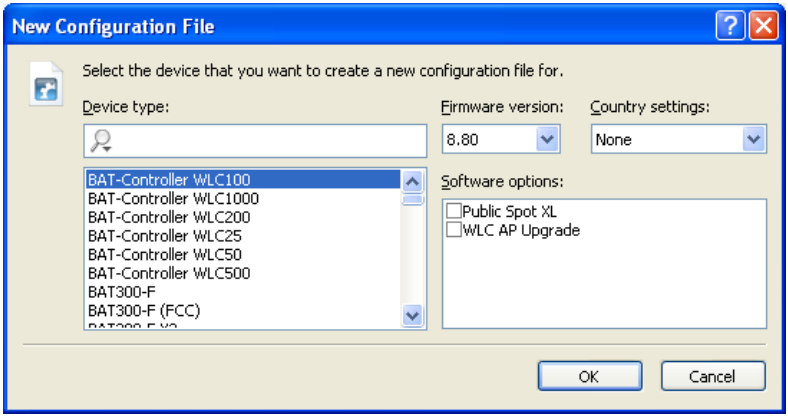
☐ In Windows Explorer, do the following:

☐ Navigate to, or create, a folder where you save the new client LANconfig file. In this example, the file is stored in the folder 'C:\LANconfig'

☐ Click the right mouse button, then select:
`New : LANconfig Configuration`

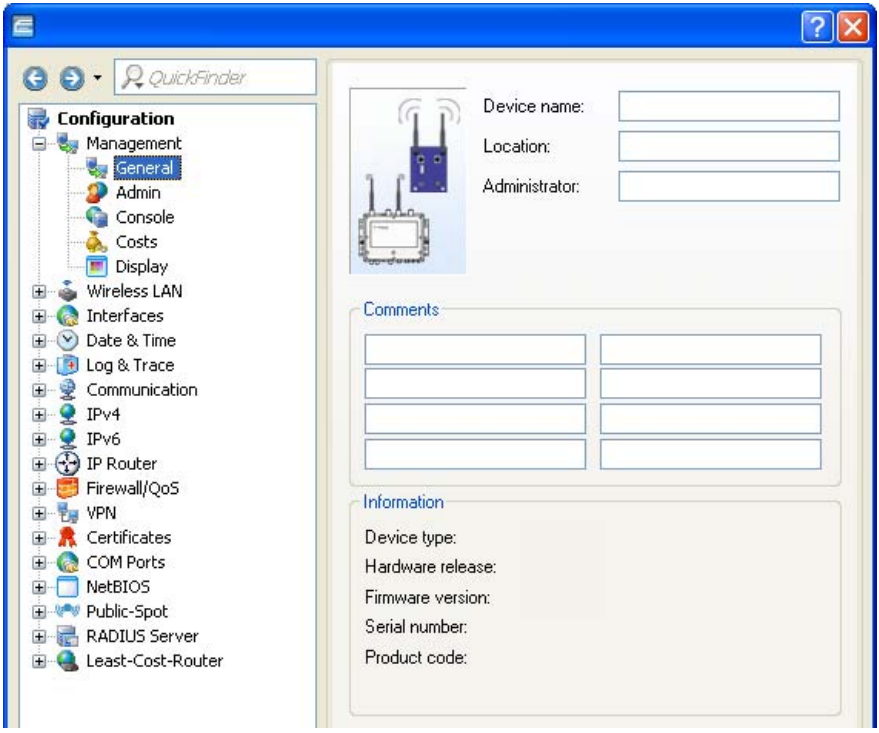
The New Configuration File dialog opens.

☐ In the 'New Configuration File' dialog, specify both the 'Device type' and the 'Firmware version' of the OpenBAT device you want to configure:



In this example, do the following:
- Device Type: Select a device.
- Firmware version: 8.80
- Country settings: Select a country. To ensure your device operates WLAN networks with the correct parameters, the device must be introduced to its national site. If you don't select any country settings, the device will allow only parameters that are permitted worldwide!
- Software options: Add configuration settings for additionally purchased software options to the basic configuration dialog by selecting its dedicated entry.
- Click 'OK'.

The following dialog opens:

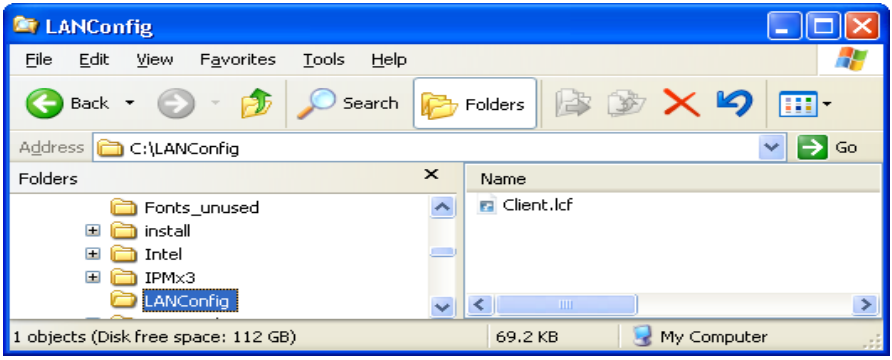


☐ Do the following:

☐ Type in a Device name. In this example, type in 'Client'.

☐ Click 'OK' to save the device configuration file.

☐ In Windows Explorer, navigate to the new file (`New LANconfig Configuration.lcf`, and change its name to `Client.lcf`:



You have created and saved a new LANconfig file. The following sections describe how to configure this file for use as a wireless client.

3.4.2 Configuring Basic Settings

Use the LANconfig Setup Wizard to configure the following basic settings for the device configuration file:

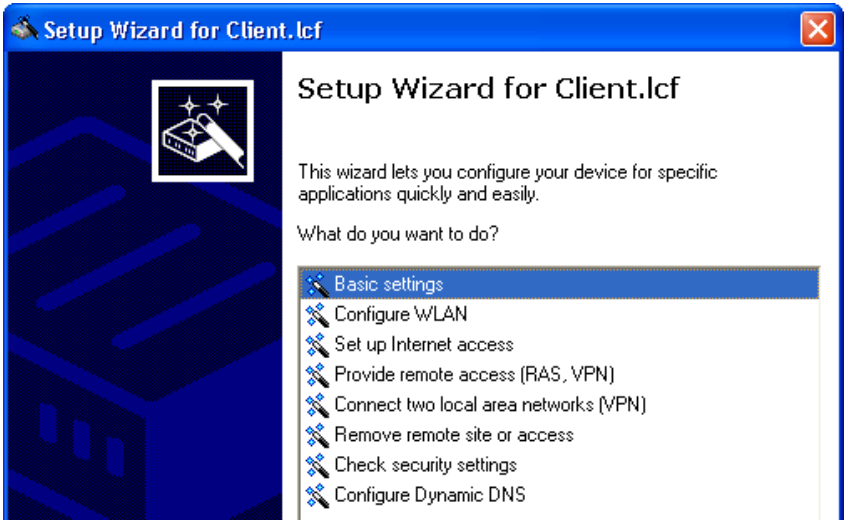
– device name
– password
– DHCP mode
– TCP/IP settings
– time synchronization settings
– optional device descriptions

☐ To start the Setup Wizard:

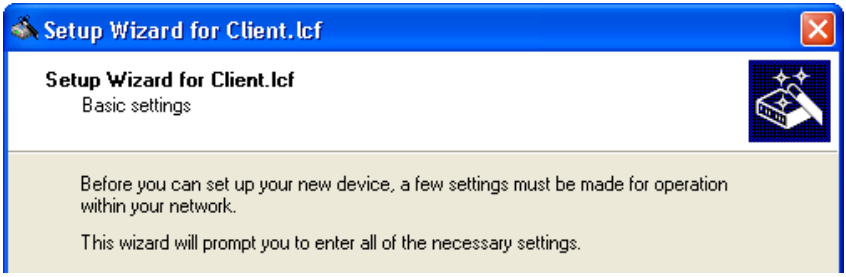
– In Windows Explorer, select the newly created LANconfig file, then

– Click the right mouse button to open a pop-up menu, then select `Setup Wizard`.

☐ In the Setup Wizard, select 'Basic settings':

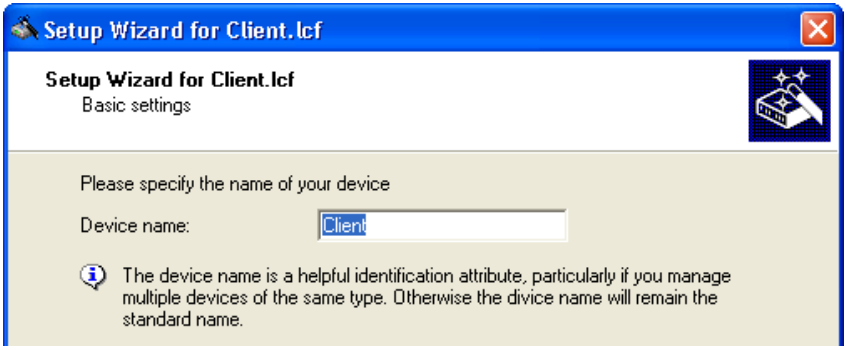

Setup Wizard for Client.lcf
Setup Wizard for Client.lcf
This wizard lets you configure your device for specific applications quickly and easily.
What do you want to do?
Basic settings
Configure WLAN
Set up Internet access
Provide remote access (RAS, VPN)
Connect two local area networks (VPN)
Remove remote site or access
Check security settings
Configure Dynamic DNS

☐ Click 'Next'. The wizard displays the following introduction:


Setup Wizard for Client.lcf
Setup Wizard for Client.lcf
Basic settings
Before you can set up your new device, a few settings must be made for operation within your network.
This wizard will prompt you to enter all of the necessary settings.

Click 'Next'.

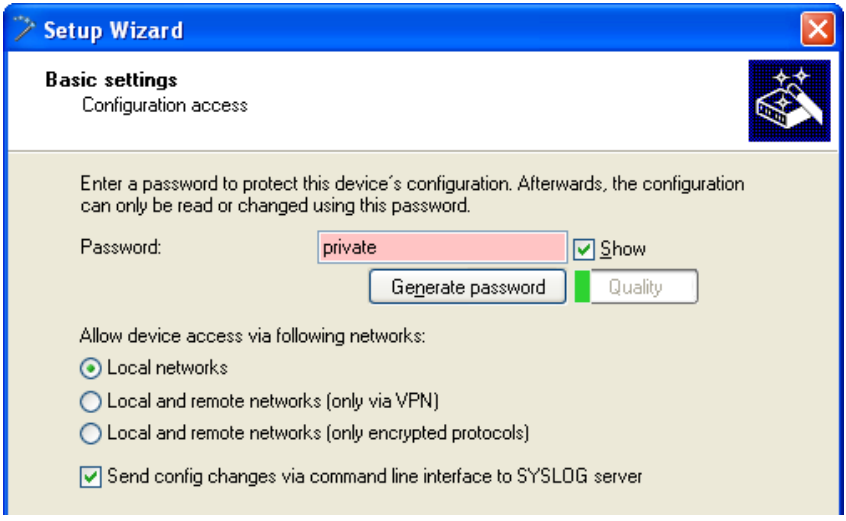
☐ Input a device name:


Setup Wizard for Client.lcf
Setup Wizard for Client.lcf
Basic settings
Please specify the name of your device
Device name:
Client
The device name is a helpful identification attribute, particularly if you manage multiple devices of the same type. Otherwise the divice name will remain the standard name.

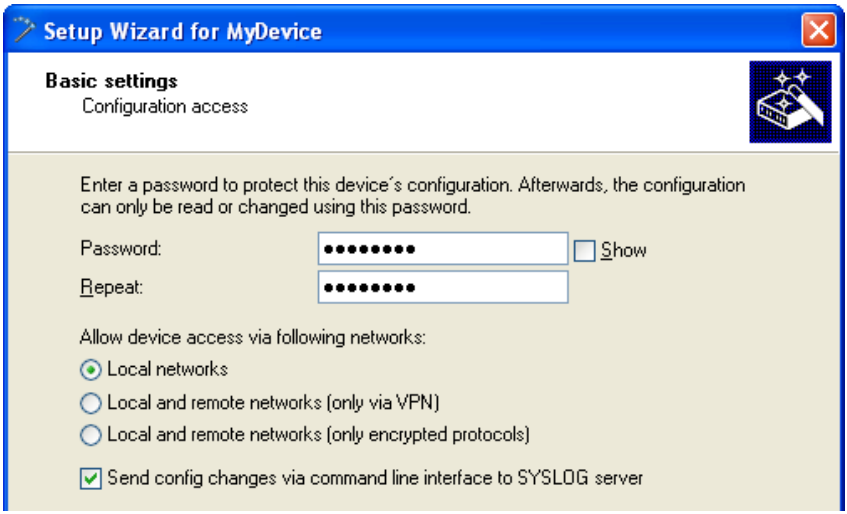
For the purpose of this example, use the name ’Client’.

☐ Click ’Next’. The following screen opens, where you need to enter a password in one of the following ways:

- Select ’Show’ (below) to display the default password (’private’) then do one of the following:
  - accept the default password
  - type in a new password
  - click ’Generate password’ to let the wizard input a new password


Setup Wizard
Basic settings
Configuration access
Enter a password to protect this device´s configuration. Afterwards, the configuration can only be read or changed using this password.
Password:
private
Show
Generate password
Quality
Allow device access via following networks:
Local networks
Local and remote networks (only via VPN)
Local and remote networks (only encrypted protocols)
Send config changes via command line interface to SYSLOG server

- De-select 'Show' (below) then either accept the default password ('private') or type in a new one. In either case, re-type the password in the 'Repeat' field.

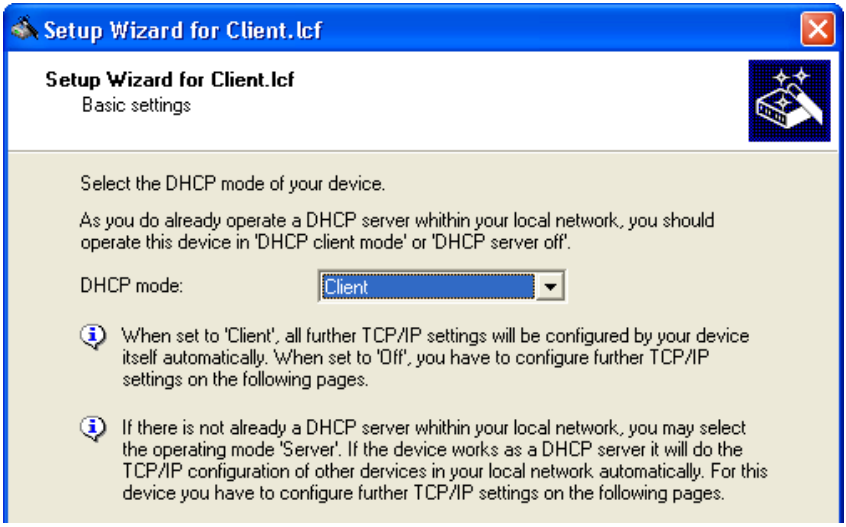

Setup Wizard for MyDevice
Basic settings
Configuration access
Enter a password to protect this device´s configuration. Afterwards, the configuration can only be read or changed using this password.
Password:
Show
Repeat:
Allow device access via following networks:
Local networks
Local and remote networks (only via VPN)
Local and remote networks (only encrypted protocols)
Send config changes via command line interface to SYSLOG server

- Set the networks permitted to access the device. If you restrict access to local networks, only PCs that are directly connected to the local area network by cable or wireless can access the device configuration.

Note: The assistent indicates the different security levels of passwords color-coded. Insecure passwords are highlighted in red, conditionally secure ones are highlighted in yellow, and secure to very secure ones are highlighted in white.

In this example, accept the default password, then click 'Next'.

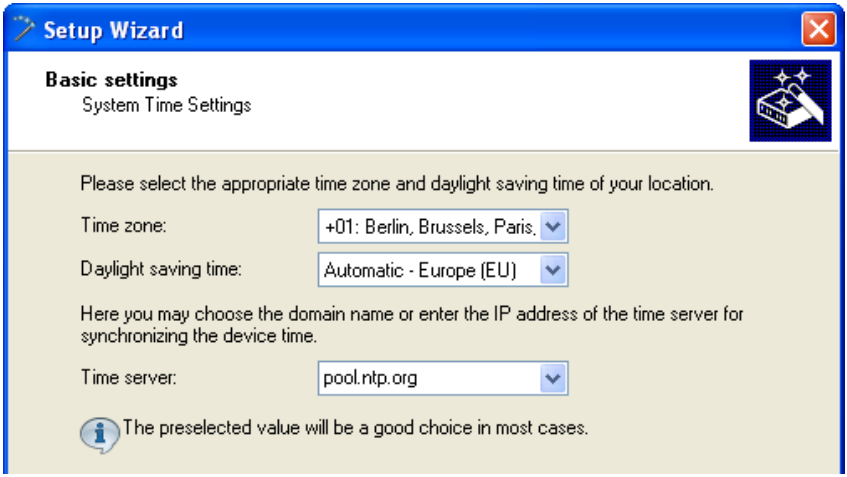
☐ Configure the OpenBAT device as DHCP client:


Setup Wizard for Client.lcf
Setup Wizard for Client.lcf
Basic settings
Select the DHCP mode of your device.
As you do already operate a DHCP server whithin your local network, you should operate this device in 'DHCP client mode' or 'DHCP server off'.
DHCP mode:
Client
When set to 'Client', all further TCP/IP settings will be configured by your device itself automatically. When set to 'Off', you have to configure further TCP/IP settings on the following pages.
If there is not already a DHCP server whithin your local network, you may select the operating mode 'Server'. If the device works as a DHCP server it will do the TCP/IP configuration of other devices in your local network automatically. For this device you have to configure further TCP/IP settings on the following pages.

When the device is turned on, it will request its IP address settings from a DHCP server on the network.

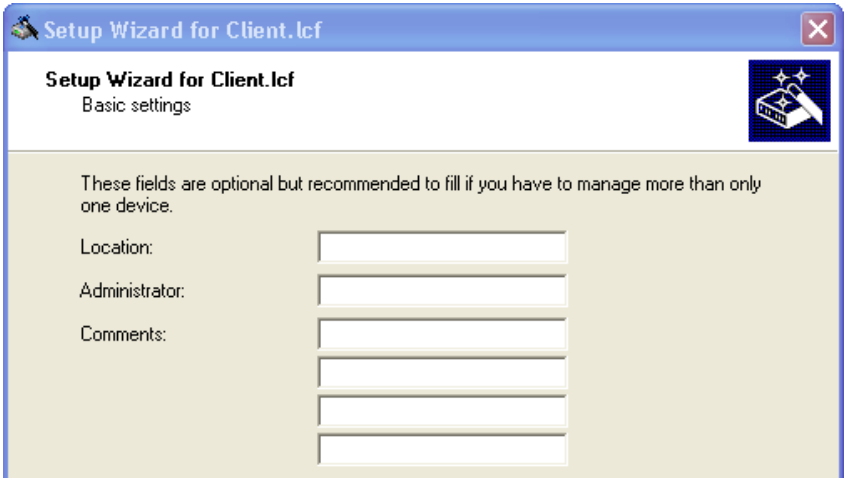
Click ’Next’.

☐ The wizard prompts you to identify your national timezone, prevailing changeover rules and a time synchronization server that will set the system time for the OpenBAT device:


Setup Wizard
Basic settings
System Time Settings
Please select the appropriate time zone and daylight saving time of your location.
Time zone:
+01: Berlin, Brussels, Paris
Daylight saving time:
Automatic - Europe (EU)
Here you may choose the domain name or enter the IP address of the time server for synchronizing the device time.
Time server:
pool.ntp.org
The preselected value will be a good choice in most cases.

Select a time server from the list, or type in its IP address.

☐ Click 'Next'. The wizard shows the following screen for optional information on the location of the device, its administrator, and any comments relating to the OpenBAT device.


Setup Wizard for Client.lcf
Setup Wizard for Client.lcf
Basic settings
These fields are optional but recommended to fill if you have to manage more than only one device.
Location:
Administrator:
Comments:

Click ’Next’.

☐ Click ’Finish’ to complete configuration of the basic settings (below):

Setup Wizard for Client.lcf
Setup Wizard for Client.lcf
You have configured all necessary basic settings required for a proper device startup.
Please select 'Finish' to apply the new settings.
The process may take about 60 seconds. After that the setup wizard restarts and further settings may be done.

3.4.3 Configuring Wireless LAN Settings

WLAN settings can be made using either the LANconfig tool's discrete configuration screens or the Setup Wizard. This task is most easily accomplished using the wizard.

☐ To start the setup wizard:

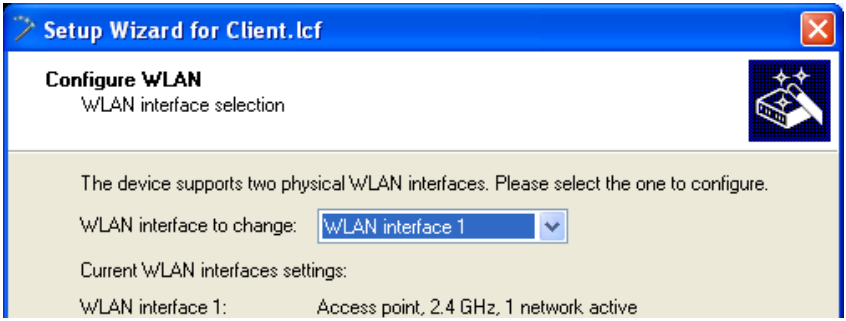
– In Windows Explorer, select the `Client.lcf` configuration file, then

– Click the right mouse button to open a pop-up menu, then select `Setup Wizard`.

☐ In the LANconfig Setup Wizard:

☐ select 'Configure WLAN'

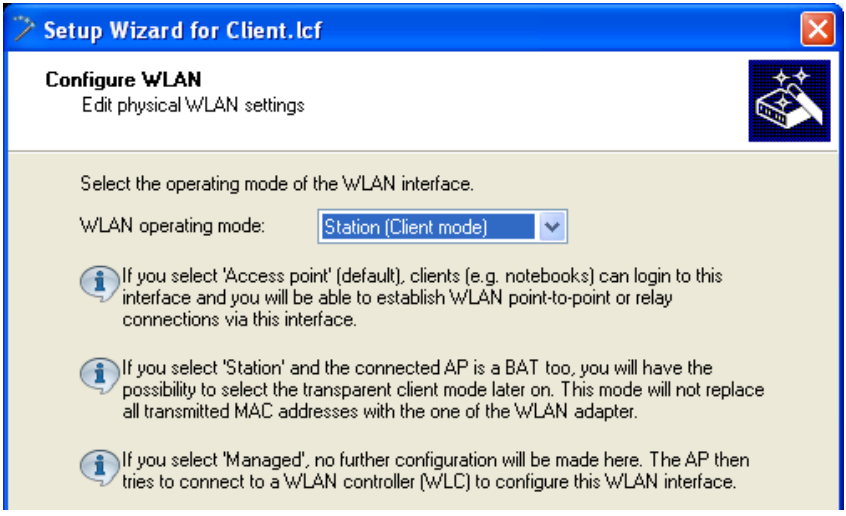
☐ click 'Next' two times, or until the wizard displays the WLAN interface selection screen


Setup Wizard for Client.lcf
Configure WLAN
WLAN interface selection
The device supports two physical WLAN interfaces. Please select the one to configure.
WLAN interface to change:
WLAN interface 1
Current WLAN interfaces settings:
WLAN interface 1:
Access point, 2.4 GHz, 1 network active

Select 'WLAN interface 1' as the 'WLAN interface to change'.

Click 'Next'.

☐ Specify an operation mode for the interface (WLAN interface 1):


Setup Wizard for Client.lcf
Configure WLAN
Edit physical WLAN settings
Select the operating mode of the WLAN interface.
WLAN operating mode:
Station (Client mode)
If you select 'Access point' (default), clients (e.g. notebooks) can login to this interface and you will be able to establish WLAN point-to-point or relay connections via this interface.
If you select 'Station' and the connected AP is a BAT too, you will have the possibility to select the transparent client mode later on. This mode will not replace all transmitted MAC addresses with the one of the WLAN adapter.
If you select 'Managed', no further configuration will be made here. The AP then tries to connect to a WLAN controller (WLC) to configure this WLAN interface.

WLAN operation modes include:

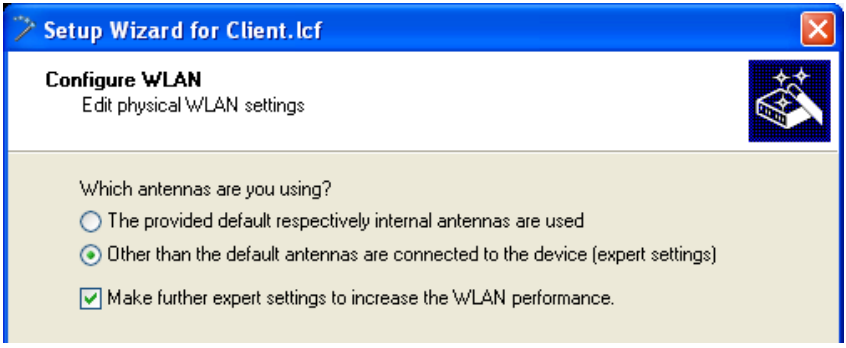
– Access Point:
The device serves as a base station, and can establish links to another access point (point-to-point), to remote clients, or to both remote access points and remote clients.

– Client:
The device serves as Client and needs to log into an Access Point. In this role, the device can link a cabled network to a WLAN over a wireless connection.

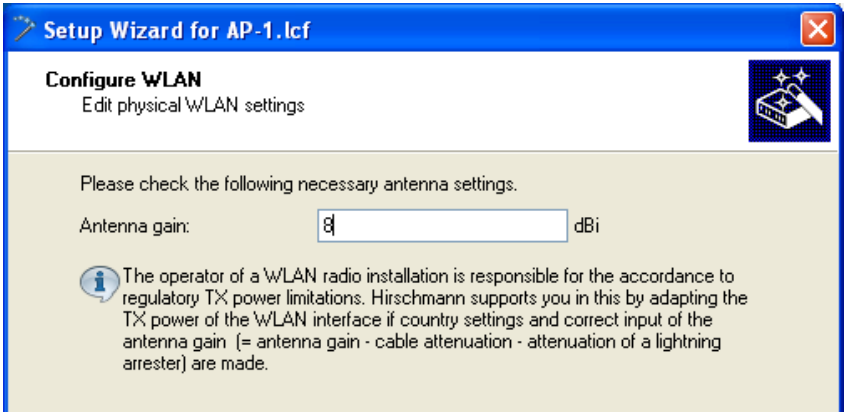
– Managed (Access point):
The device operates as an Access point, but searches for a central WLAN controller it can obtain a configuration from.

Select 'Client', then click 'Next'.

☐ Check the antenna settings:

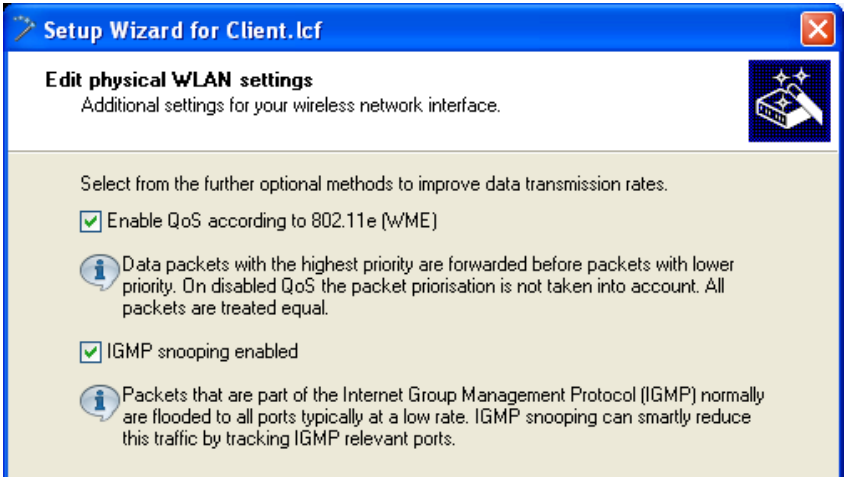

Setup Wizard for Client.lcf
Configure WLAN
Edit physical WLAN settings
Which antennas are you using?
The provided default respectively internal antennas are used
Other than the default antennas are connected to the device (expert settings)
Make further expert settings to increase the WLAN performance.

☐ Check the antenna settings:


Setup Wizard for AP-1.lcf
Configure WLAN
Edit physical WLAN settings
Please check the following necessary antenna settings.
Antenna gain:
8
dBi
The operator of a WLAN radio installation is responsible for the accordance to regulatory TX power limitations. Hirschmann supports you in this by adapting the TX power of the WLAN interface if country settings and correct input of the antenna gain (= antenna gain - cable attenuation - attenuation of a lightning arrester) are made.

the calculated antenna gain is 8 dBi for this example

☐ Click 'Next'.
The wizard presents settings that can be used to increase data transmission rates:


Setup Wizard for Client.lcf
Edit physical WLAN settings
Additional settings for your wireless network interface.
Select from the further optional methods to improve data transmission rates.
Enable QoS according to 802.11e (WME)
Data packets with the highest priority are forwarded before packets with lower priority. On disabled QoS the packet priorisation is not taken into account. All packets are treated equal.
IGMP snooping enabled
Packets that are part of the Internet Group Management Protocol (IGMP) normally are flooded to all ports typically at a low rate. IGMP snooping can smartly reduce this traffic by tracking IGMP relevant ports.

You can enable or disable the following services:

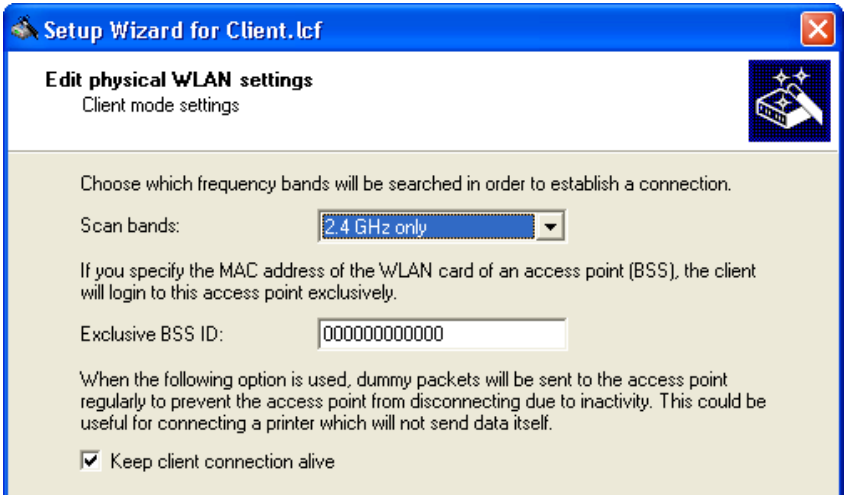
– QoS

– IGMP Snooping

For the purpose of this example, all available data rate enhancing options are selected.

Click 'Next'.

☐ The wizard presents the following screen:


Setup Wizard for Client.lcf
Edit physical WLAN settings
Client mode settings
Choose which frequency bands will be searched in order to establish a connection.
Scan bands:
2.4 GHz only
If you specify the MAC address of the WLAN card of an access point (BSS), the client will login to this access point exclusively.
Exclusive BSS ID:
000000000000
When the following option is used, dummy packets will be sent to the access point regularly to prevent the access point from disconnecting due to inactivity. This could be useful for connecting a printer which will not send data itself.
Keep client connection alive

In this screen, enter settings for the following fields:

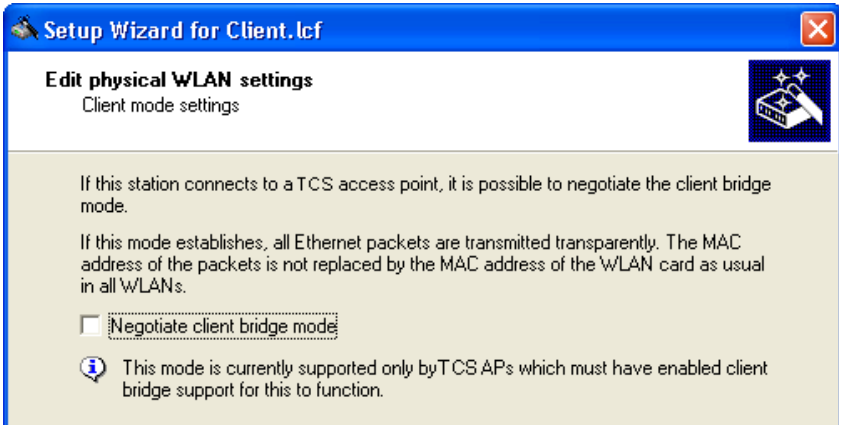
– Scan bands: Select the frequency bands to be scanned by the client when it attempts to establish a connection. In this example, select '2.4 GHz only'.

– Exclusive BSS ID: If you want the client to connect to a specific access point, type in its MAC address. In this example, type in a value consisting exclusively of zeroes, indicating no device is specified, to configure a roaming client.

– Select 'Keep client connection alive'.

Click ’Next’.

☐ De-select the ’Negotiate client bridge mode’ option, below:


Setup Wizard for Client.lcf
Edit physical WLAN settings
Client mode settings
If this station connects to a TCS access point, it is possible to negotiate the client bridge mode.
If this mode establishes, all Ethernet packets are transmitted transparently. The MAC address of the packets is not replaced by the MAC address of the WLAN card as usual in all WLANs.
Negotiate client bridge mode
This mode is currently supported only byTCS APs which must have enabled client bridge support for this to function.

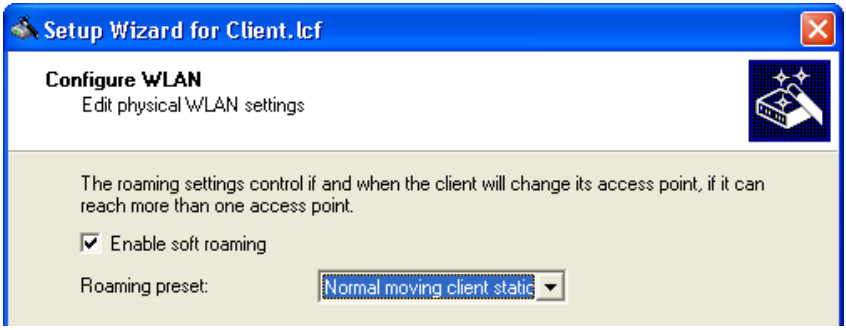
Client bridge support relates to a network design that consists of:

– an OpenBAT device in the role of Access Point
– an OpenBAT device in the role of Client
– one or more remote Ethernet devices connected to the Client OpenBAT device in Client mode

Typically, packets sent from a remote Ethernet device to the access point via the wireless client contain the MAC address of just the wireless client. Enabling client bridge support also includes in the packet the MAC address of the remote device.

For this example, de-select ’Negotiate client bridge mode’, then click ’Next’.

☐ Use the next screen to enable soft roaming for the client:


Setup Wizard for Client.lcf
Configure WLAN
Edit physical WLAN settings
The roaming settings control if and when the client will change its access point, if it can reach more than one access point.
Enable soft roaming
Roaming preset:
Normal moving client static

Enabling soft roaming helps provide a seamless transition for a wireless client when it roams between access points. Do the following:

– Select ’Enable soft roaming’

– Set the Roaming preset field to ’Normal moving client station’.

Click ’Next’.

☐ Enter the Network name (also known as the Service Set Identifier or ’SSID’):

Setup Wizard for Client.lcf
Configure WLAN
Edit WLAN network
Enter the network name of your wireless network.
This network name is provided by an access point for the wireless network that this device should connect to.
Network name (SSID):
Company_1

For the purpose of this example, use the SSID ’Company_1’.

Click ’Next’.

☐ Specify the transmission encryption protocol:

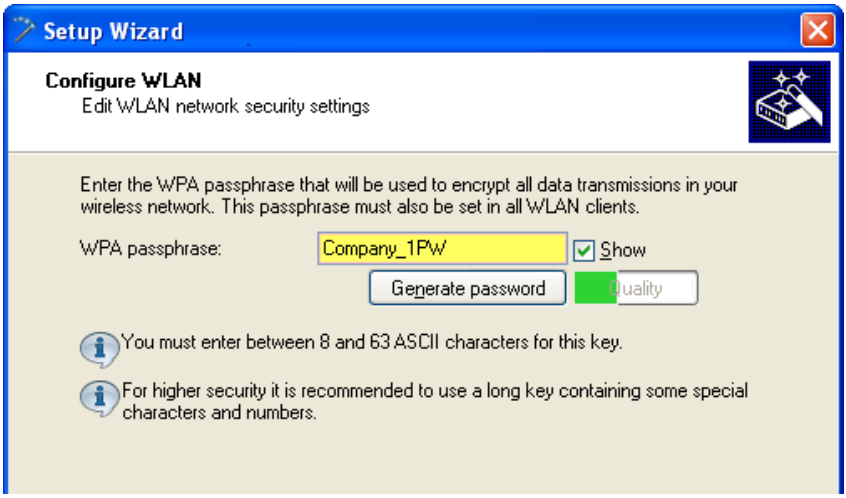
Setup Wizard for Client.lcf
Configure WLAN
Edit WLAN network security settings
Activate encryption for your wireless network to allow access only to authorized clients and encrypt all data transmissions.
Use WPA-2 (802.11i) Enhanced Security with Advanced Encryption Standard (WPA/AES) for encryption
Use WEP (Wired Equivalent Privacy) for encryption (not recommended!)
Do not activate encryption for the wireless LAN (only for public access)

Note: Use WPA-2 for increased security.

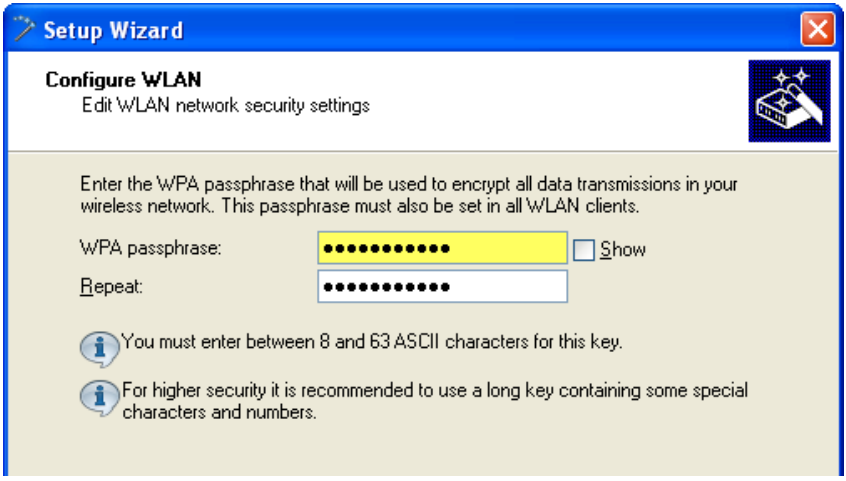
Click 'Next'.

☐ The following screen opens, where you need to enter a WPA passphrase in one of the following ways:

– Select 'Show' (below), then do one of the following:
  - type in a new WPA passphrase
  - click 'Generate password' to let the wizard input a new passphrase

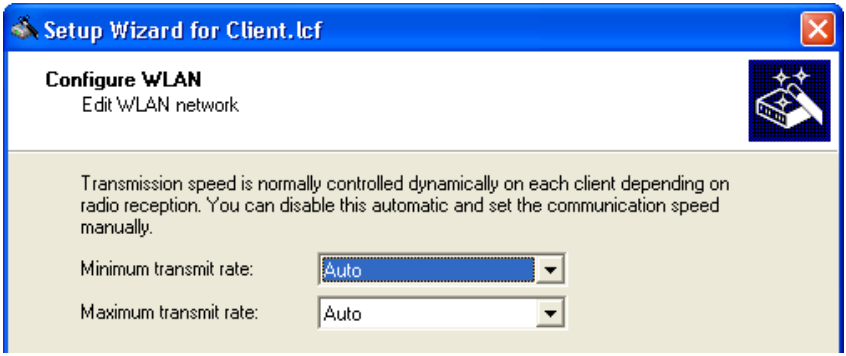

Setup Wizard
Configure WLAN
Edit WLAN network security settings
Enter the WPA passphrase that will be used to encrypt all data transmissions in your wireless network. This passphrase must also be set in all WLAN clients.
WPA passphrase:
Company_1PW
Show
Generate password
Quality
You must enter between 8 and 63 ASCII characters for this key.
For higher security it is recommended to use a long key containing some special characters and numbers.

– De-select 'Show' (below) then type in a new WPA passphrase. In this case, re-type the password in the 'Repeat' field:


Setup Wizard
Configure WLAN
Edit WLAN network security settings
Enter the WPA passphrase that will be used to encrypt all data transmissions in your wireless network. This passphrase must also be set in all WLAN clients.
WPA passphrase:
Show
Repeat:
You must enter between 8 and 63 ASCII characters for this key.
For higher security it is recommended to use a long key containing some special characters and numbers.

In this example, type in the passphrase 'CompanyPW', then click 'Next'.

☐ Specify how transmission speed between the wireless client and any access point will be determined:

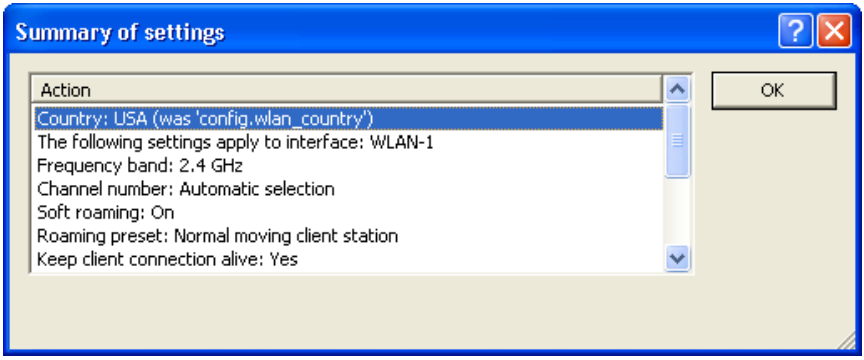

Setup Wizard for Client.lcf
Configure WLAN
Edit WLAN network
Transmission speed is normally controlled dynamically on each client depending on radio reception. You can disable this automatic and set the communication speed manually.
Minimum transmit rate:
Auto
Maximum transmit rate:
Auto

Select 'Auto' for both the Minimum transmit rate and the Maximum transmit rate, then click 'Next'.

☐ You are now ready to complete the configuration of the wireless client:

Setup Wizard for Client.lcf
Setup Wizard for Client.lcf
You have successfully changed the WLAN settings.
Open the following table to get an overview of the changes made.
Summary of settings...
Select 'Finish' to apply the new settings.

☐ Click on the 'Summary of settings...' button to display a list of all configuration settings for the wireless client device:

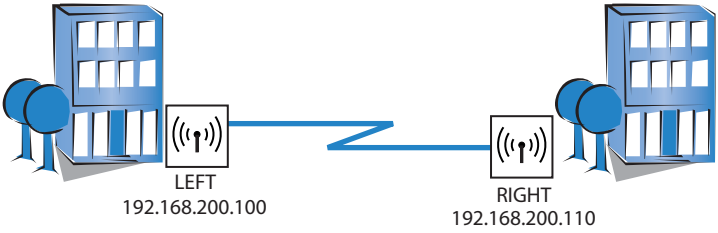


Click ’OK’ to close the Summary window.

Click ’Finish’ to complete the wizard and save the settings for this wireless client.

3.5 WLAN Bridge: Single Subnet

This example shows how to configure two OpenBAT devices as Access Points to form a point-to-point WLAN bridge connecting two segments of the same subnet. Each Access Point is configured to allow access only by its direct bridge partner. None of the devices is configured to provide routing functionality.



The significant configuration settings for each device are as follows:

Station Name:	LEFT	RIGHT
Role:	Access Point	Access Point
IP address:	192,168,200,100	192,168,200,110
Subnet Mask:	255.255.255.0	255.255.255.0
Channel Selection Scheme	Master	Slave
Point-to-Point Partner	RIGHT	LEFT

3.5.1 Configuring the LEFT Device

Create a new device configuration file using either the LANconfig software's individual configuration pages or its Setup Wizard. The easier approach is to use the Setup Wizard to configure the following groups device settings:

- Basic Settings
- WLAN Settings

Configuring Basic Settings

After you have created a new configuration file (see on page 44), the next task is to input the basic Ethernet communication settings for the OpenBAT devices. Basic settings include:

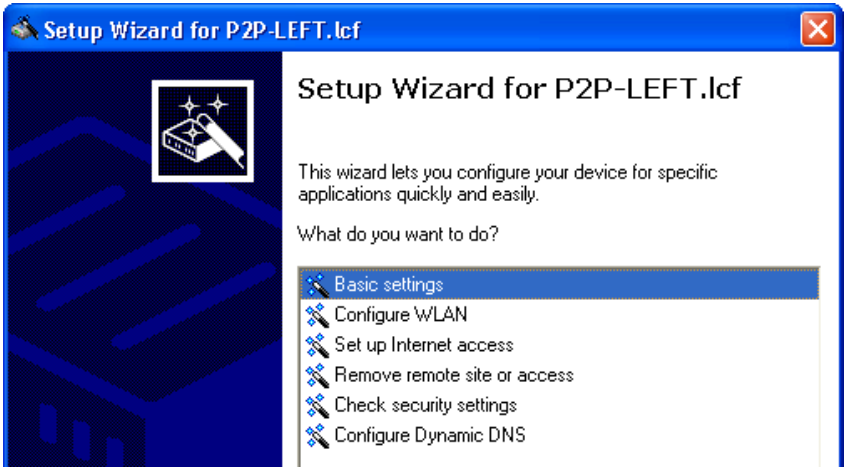
– device name
– password
– DHCP mode
– TCP/IP settings
– time synchronization settings
– optional device descriptions

☐ In Windows Explorer, do the following:

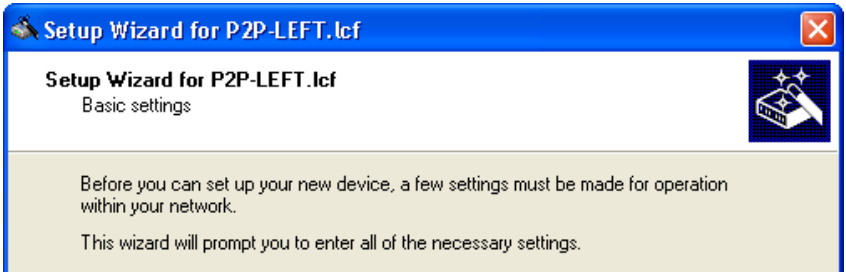
– Select the configuration file.
– Click the right mouse button and select `Rename`.
– Type in a new name for the file: `P2P-LEFT.lcf`.

☐ To start the Setup Wizard, click the right mouse button to open a pop-up menu, then select `Setup Wizard`.

☐ In the Setup Wizard, select 'Basic settings':

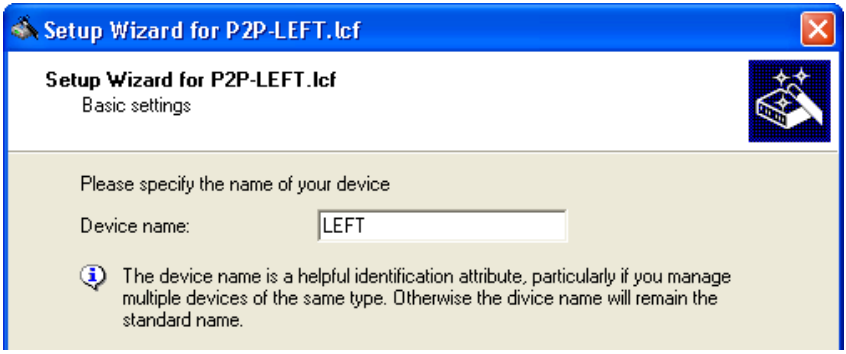

Setup Wizard for P2P-LEFT.lcf
Setup Wizard for P2P-LEFT.lcf
This wizard lets you configure your device for specific applications quickly and easily.
What do you want to do?
Basic settings
Configure WLAN
Set up Internet access
Remove remote site or access
Check security settings
Configure Dynamic DNS

Click 'Next'. The wizard displays the following introduction:


Setup Wizard for P2P-LEFT.lcf
Setup Wizard for P2P-LEFT.lcf
Basic settings
Before you can set up your new device, a few settings must be made for operation within your network.
This wizard will prompt you to enter all of the necessary settings.

☐ Click ‘Next’.

☐ Confirm the device name:

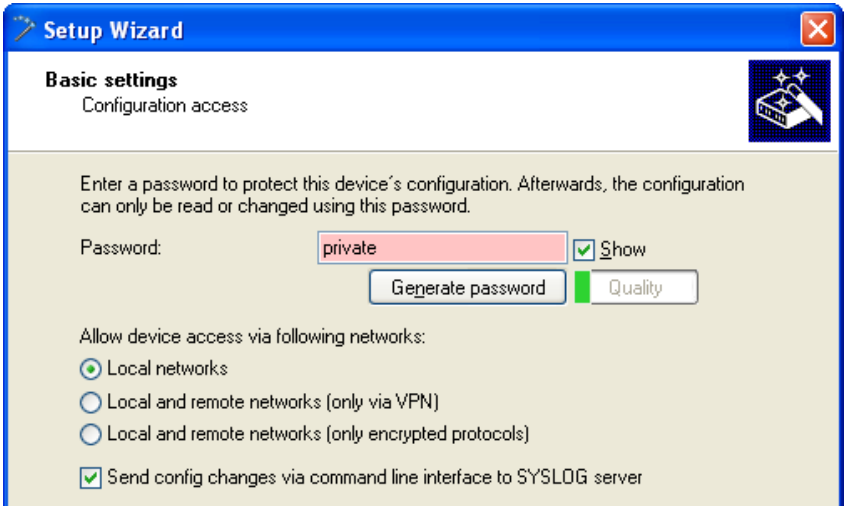

Setup Wizard for P2P-LEFT.lcf
Setup Wizard for P2P-LEFT.lcf
Basic settings
Please specify the name of your device
Device name:
LEFT
The device name is a helpful identification attribute, particularly if you manage multiple devices of the same type. Otherwise the divice name will remain the standard name.

The wizard displays the Device name you previously input (’LEFT’).

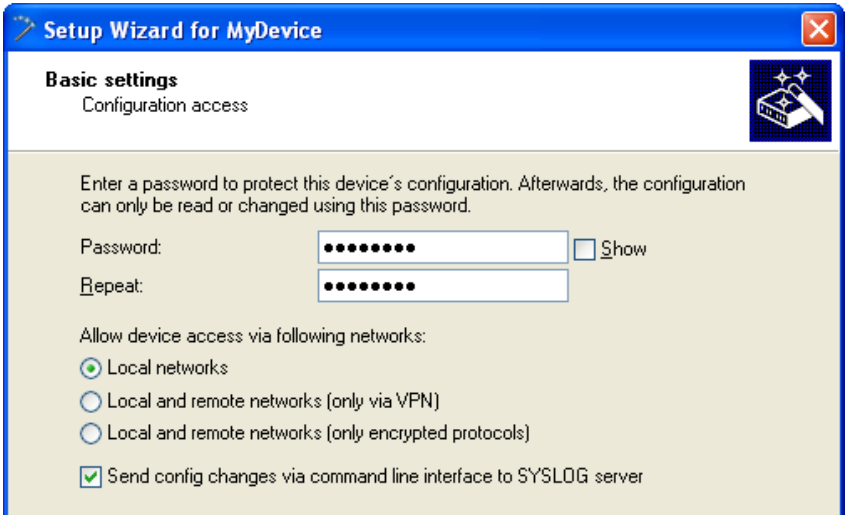
Note: The default device name is a concatenation of the device part number and the last 3 octets of the device MAC address.

☐ Click 'Next'. The following screen opens, where you need to enter a password in one of the following ways:

- Select 'Show' (below) to display the default password ('private') then do one of the following:
  - accept the default password
  - type in a new password
  - click 'Generate password' to let the wizard input a new password


Setup Wizard
Basic settings
Configuration access
Enter a password to protect this device´s configuration. Afterwards, the configuration can only be read or changed using this password.
Password:
private
Show
Generate password
Quality
Allow device access via following networks:
Local networks
Local and remote networks (only via VPN)
Local and remote networks (only encrypted protocols)
Send config changes via command line interface to SYSLOG server

- De-select 'Show' (below) then either accept the default password ('private') or type in a new one. In either case, re-type the password in the 'Repeat' field.

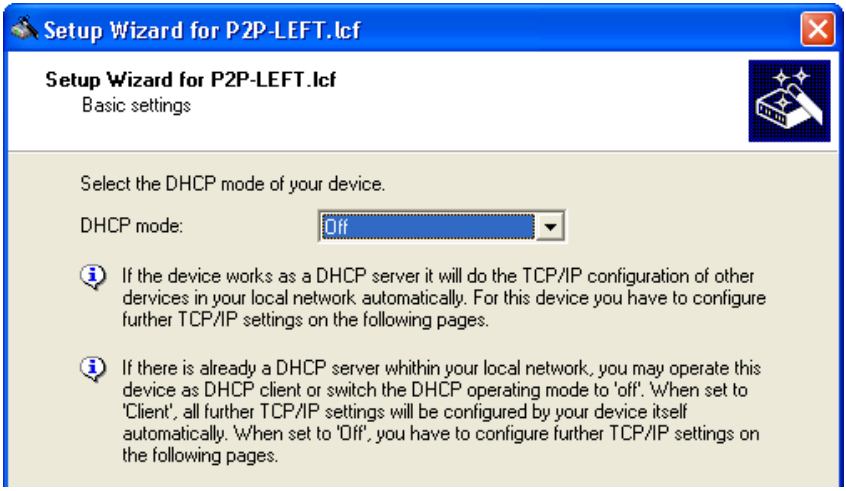

Setup Wizard for MyDevice
Basic settings
Configuration access
Enter a password to protect this device´s configuration. Afterwards, the configuration can only be read or changed using this password.
Password:
Show
Repeat:
Allow device access via following networks:
Local networks
Local and remote networks (only via VPN)
Local and remote networks (only encrypted protocols)
Send config changes via command line interface to SYSLOG server

- Set the networks permitted to access the device. If you restrict access to local networks, only PCs that are directly connected to the local area network by cable or wireless can access the device configuration.

Note: The assistent indicates the different security levels of passwords color-coded. Insecure passwords are highlighted in red, conditionally secure ones are highlighted in yellow, and secure to very secure ones are highlighted in white.

In this example, accept the default password, then click ’Next’.

☐ Define the DHCP mode of the OpenBAT device:


Setup Wizard for P2P-LEFT.lcf
Setup Wizard for P2P-LEFT.lcf
Basic settings
Select the DHCP mode of your device.
DHCP mode:
Off
If the device works as a DHCP server it will do the TCP/IP configuration of other devices in your local network automatically. For this device you have to configure further TCP/IP settings on the following pages.
If there is already a DHCP server whithin your local network, you may operate this device as DHCP client or switch the DHCP operating mode to 'off'. When set to 'Client', all further TCP/IP settings will be configured by your device itself automatically. When set to 'Off', you have to configure further TCP/IP settings on the following pages.

Select one of the following DHCP modes:

– Off:
  The device functions neither as DHCP client nor as DHCP server. In this mode, you need to manually input the IP address settings.

– Server:
  The OpenBAT device functions as DHCP server, and assigns IP address settings to other network devices.

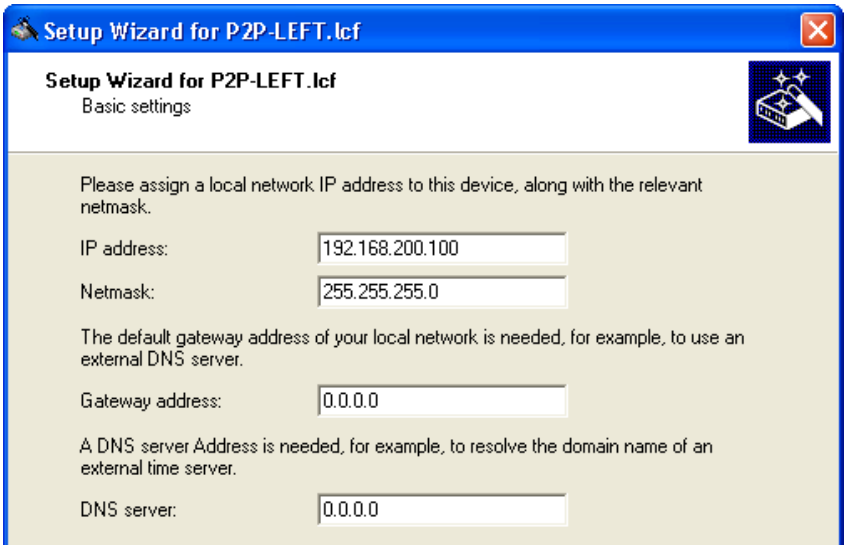
– Client:
  This setting causes the OpenBAT device to request the IP address settings from a DHCP server on the network.

If a DHCP server exists on your network, select the ‘DHCP mode’ of ‘Off’. The default ‘DHCP mode’ setting of ‘Client’ can override a manually assigned IP address.

Note: Your DHCP mode selection determines the next screen displayed by the Setup Wizard.

Click ‘Next’.

- If you selected 'Off' for the DHCP mode, manually input the TCP/IP settings for the OpenBAT device:


Setup Wizard for P2P-LEFT.lcf
Setup Wizard for P2P-LEFT.lcf
Basic settings
Please assign a local network IP address to this device, along with the relevant netmask.
IP address:
192.168.200.100
Netmask:
255.255.255.0
The default gateway address of your local network is needed, for example, to use an external DNS server.
Gateway address:
0.0.0.0
A DNS server Address is needed, for example, to resolve the domain name of an external time server.
DNS server:
0.0.0.0

Enter values for both the ’IP address’ and the ’Netmask’.
For the purpose of this example, these settings are:

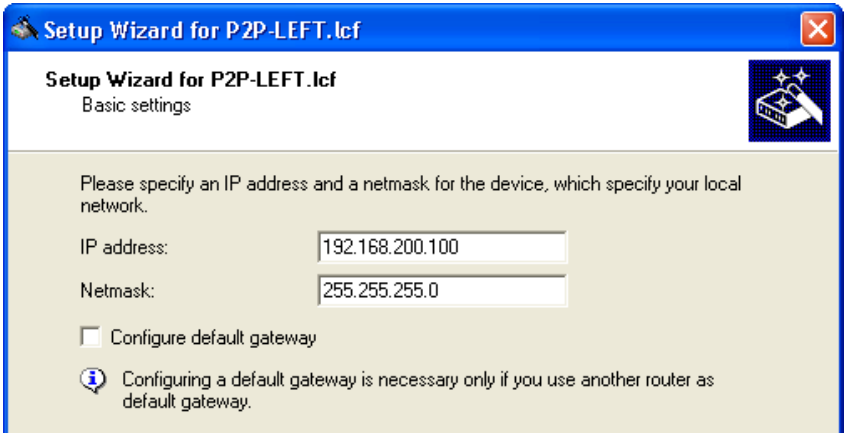
– IP address: 192.168.200.10

– Netmask: 255.255.255.0

Note: For a point-to-point link, settings for Gateway address and DNS server are not required.

Click ‘Next’.

- If you selected ’Server’ for the DHCP mode, the wizard displays the following screen for TCP/IP settings:


Setup Wizard for P2P-LEFT.lcf
Setup Wizard for P2P-LEFT.lcf
Basic settings
Please specify an IP address and a netmask for the device, which specify your local network.
IP address:
192.168.200.100
Netmask:
255.255.255.0
Configure default gateway
Configuring a default gateway is necessary only if you use another router as default gateway.

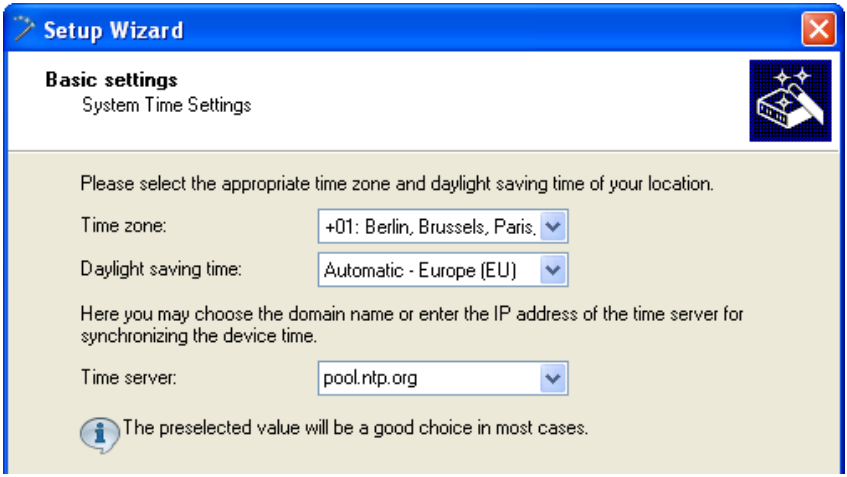
Do the following:

☐ Enter values for the ’IP address’ and ’Netmask’.

☐ For a point-to-point link, settings for ‘Gateway address’ and ‘DNS server’ are not required.

☐ Click ’Next’.

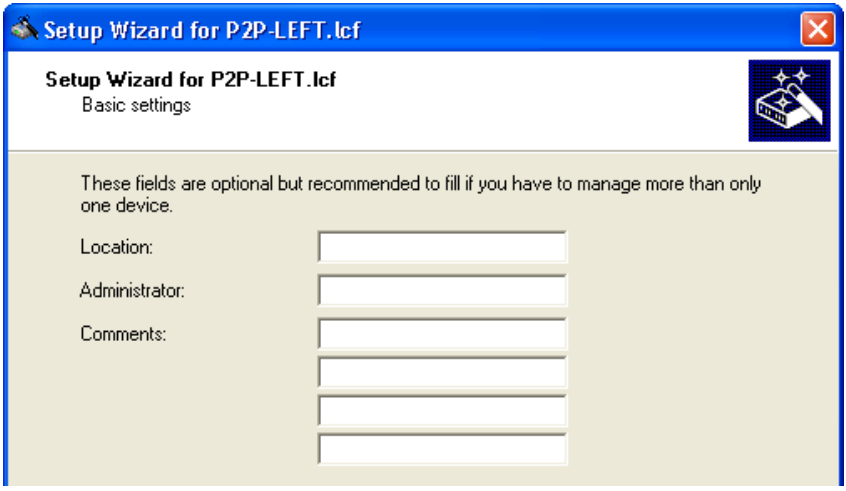
☐ The wizard prompts you to identify your national timezone, prevailing changeover rules and a time synchronization server that will set the system time for the OpenBAT device:


Setup Wizard
Basic settings
System Time Settings
Please select the appropriate time zone and daylight saving time of your location.
Time zone:
+01: Berlin, Brussels, Paris
Daylight saving time:
Automatic - Europe (EU)
Here you may choose the domain name or enter the IP address of the time server for synchronizing the device time.
Time server:
pool.ntp.org
The preselected value will be a good choice in most cases.

Select a time server from the list, or type in its IP address.

Click 'Next'.

☐ The wizard shows the following screen for optional information on the location of the device, its administrator, and any comments relating to the OpenBAT device.


Setup Wizard for P2P-LEFT.lcf
Setup Wizard for P2P-LEFT.lcf
Basic settings
These fields are optional but recommended to fill if you have to manage more than only one device.
Location:
Administrator:
Comments:

Click ‘Next’.

☐ Click 'Finish' to complete the configuration of the basic settings (below):

Setup Wizard for P2P-LEFT.lcf
Setup Wizard for P2P-LEFT.lcf
You have configured all necessary basic settings required for a proper device startup.
Please select 'Finish' to apply the new settings.
The process may take about 60 seconds. After that the setup wizard restarts and further settings may be done.

Configuring WLAN Settings

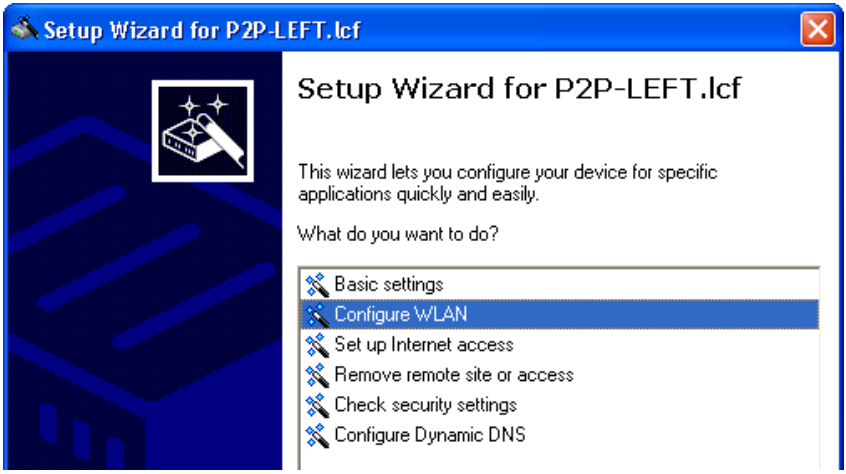
WLAN settings can be made using either the LANconfig tool’s discrete configuration screens or the Setup Wizard. This task is most easily accomplished using the wizard.

☐ To start the Setup Wizard:

– In Windows Explorer, select the `P2P-LEFT.lcf` LANconfig file, then

– Click the right mouse button to open a pop-up menu, then select `Setup Wizard`.

☐ In the wizard, select ’Configure WLAN’ (below):


Setup Wizard for P2P-LEFT.lcf
Setup Wizard for P2P-LEFT.lcf
This wizard lets you configure your device for specific applications quickly and easily.
What do you want to do?
Basic settings
Configure WLAN
Set up Internet access
Remove remote site or access
Check security settings
Configure Dynamic DNS

Click ‘Next’.

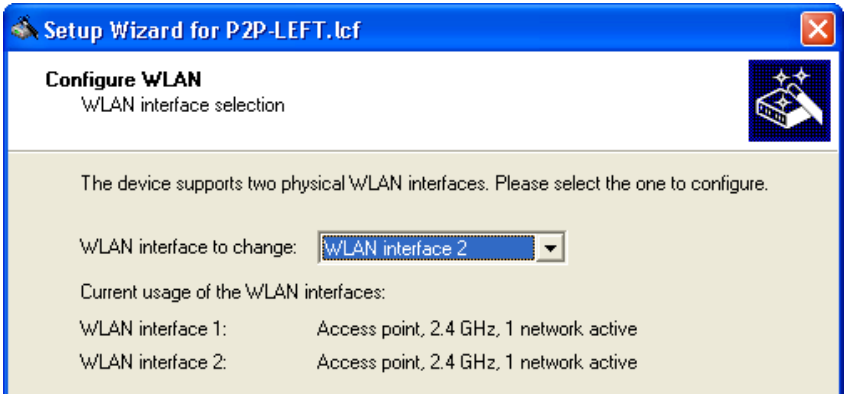
☐ Select the country in which the OpenBAT device is operated:

Setup Wizard for P2P-LEFT.lcf
Configure WLAN
Edit physical WLAN settings
The device must know its country location in order to use the correct wireless base settings.
Please select the country in which the device will be operated.
Country:
USA

Note: The country designation determines both the available frequency bands, and the limits for output power considered by the device.

Click ‘Next’.

☐ The wizard prompts you to select a WLAN interface to configure:

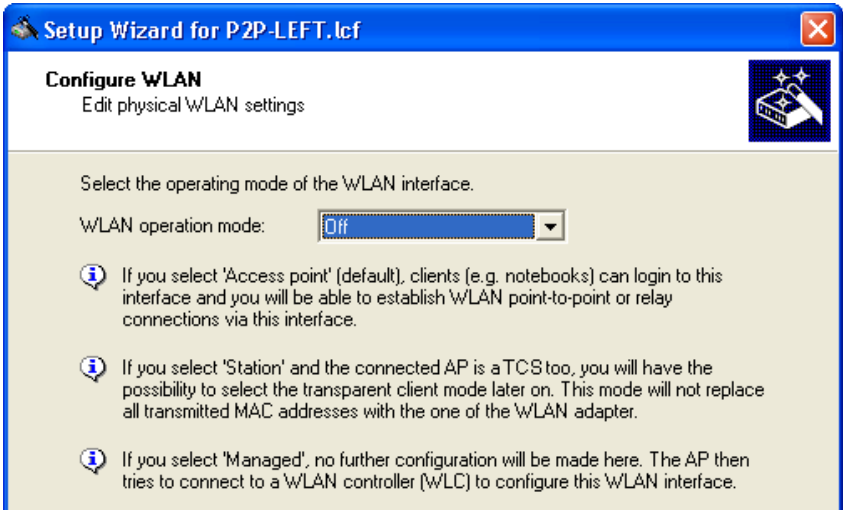

Setup Wizard for P2P-LEFT.lcf
Configure WLAN
WLAN interface selection
The device supports two physical WLAN interfaces. Please select the one to configure.
WLAN interface to change:
WLAN interface 2
Current usage of the WLAN interfaces:
WLAN interface 1:
Access point, 2.4 GHz, 1 network active
WLAN interface 2:
Access point, 2.4 GHz, 1 network active

A device can have multiple WLAN interfaces. Here, the selected device has two interfaces. By default, both interfaces are enabled.

Note: You can configure just one WLAN interface at a time. After selecting interface 2, proceed through the wizard's remaining pages and finish configuration for that interface. Next, re-start the Configure WLAN wizard and configure interface 1.

Select 'WLAN interface 2' as the WLAN interface to configure, then click 'Next'.

☐ The next step is to enable or disable the selected WLAN interface:

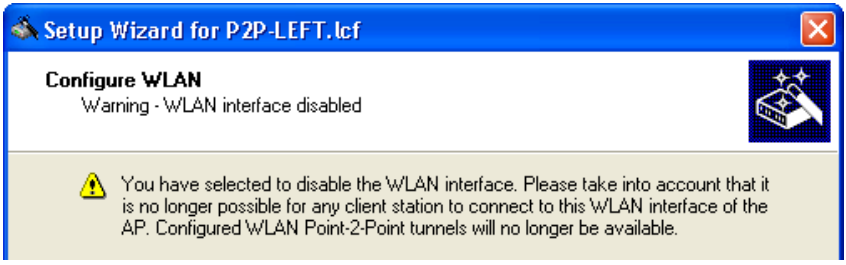

Setup Wizard for P2P-LEFT.lcf
Configure WLAN
Edit physical WLAN settings
Select the operating mode of the WLAN interface.
WLAN operation mode:
Off
If you select 'Access point' (default), clients (e.g. notebooks) can login to this interface and you will be able to establish WLAN point-to-point or relay connections via this interface.
If you select 'Station' and the connected AP is a TCS too, you will have the possibility to select the transparent client mode later on. This mode will not replace all transmitted MAC addresses with the one of the WLAN adapter.
If you select 'Managed', no further configuration will be made here. The AP then tries to connect to a WLAN controller (WLC) to configure this WLAN interface.

A point-to-point WLAN bridge requires just one interface. In this example, the currently selected interface—WLAN interface 2—will be disabled. (You will later configure WLAN interface 1 to support the point-to-point WLAN bridge.

Disable WLAN interface 2 by setting its 'WLAN operation mode' to 'Off'.

Click 'Next'.

☐ The wizard notifies you that you are about to disable interface 2:


Setup Wizard for P2P-LEFT.lcf
Configure WLAN
Warning - WLAN interface disabled
You have selected to disable the WLAN interface. Please take into account that it is no longer possible for any client station to connect to this WLAN interface of the AP. Configured WLAN Point-2-Point tunnels will no longer be available.

Click ‘Next’.

☐ Complete the configuration of WLAN interface 2:

Setup Wizard for P2P-LEFT.lcf
Setup Wizard for P2P-LEFT.lcf
You have successfully changed the WLAN settings.
Open the following table to get an overview of the changes made.
Summary of settings...
Select 'Finish' to apply the new settings.

Click ’Finish’.

☐ Return to the Windows Explorer folder where the file LANconfig file is saved, then do the following:

– select the LANconfig file (`AP-1.lcf`)

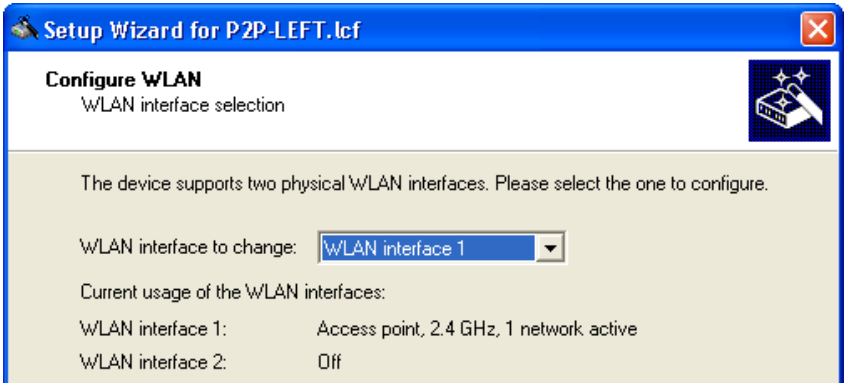
– click the right mouse button to open a pop-up menu

– select `Setup Wizard`

☐ In the LANconfig Setup Wizard:

– select ’Configure WLAN’

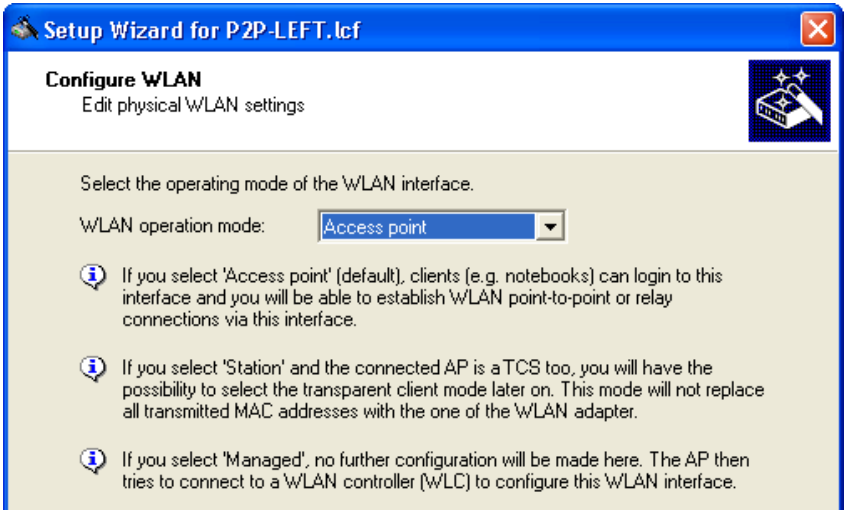
– click ’Next’ two times, or until the wizard displays the WLAN interface selection screen


Setup Wizard for P2P-LEFT.lcf
Configure WLAN
WLAN interface selection
The device supports two physical WLAN interfaces. Please select the one to configure.
WLAN interface to change:
WLAN interface 1
Current usage of the WLAN interfaces:
WLAN interface 1:
Access point, 2.4 GHz, 1 network active
WLAN interface 2:
Off

Note: This screen indicates that WLAN interface 2 has been turned off. The next step is to configure WLAN interface 1.

Select 'WLAN interface 1' for the configuration and click 'Next'.

☐ Specify an operation mode for the interface (WLAN interface 1):


Setup Wizard for P2P-LEFT.lcf
Configure WLAN
Edit physical WLAN settings
Select the operating mode of the WLAN interface.
WLAN operation mode:
Access point
If you select 'Access point' (default), clients (e.g. notebooks) can login to this interface and you will be able to establish WLAN point-to-point or relay connections via this interface.
If you select 'Station' and the connected AP is a TCS too, you will have the possibility to select the transparent client mode later on. This mode will not replace all transmitted MAC addresses with the one of the WLAN adapter.
If you select 'Managed', no further configuration will be made here. The AP then tries to connect to a WLAN controller (WLC) to configure this WLAN interface.

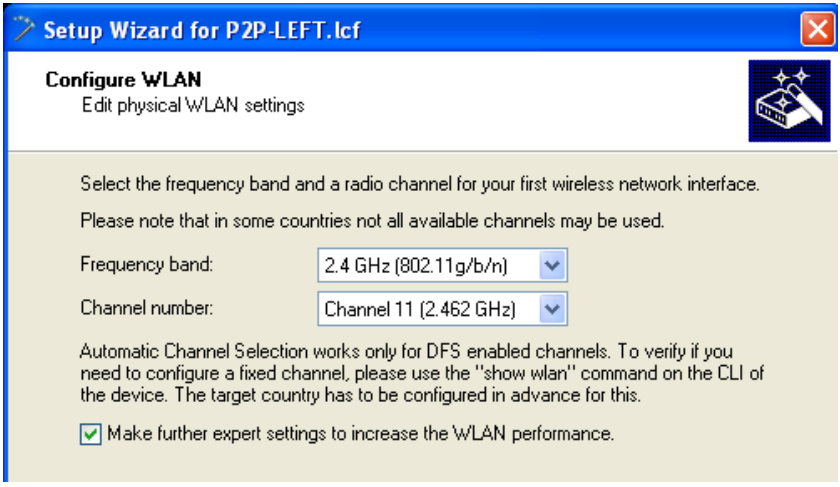
WLAN operation modes include:

– Access Point:
  The device serves as Access Point and can establish connections to other Access Points (point-to-point), to remote clients, or to both Access Points and Clients.

– Client:
  The device serves as Client and needs to log into an Access Point. In this role, the device can connect a cabled network to a WLAN over a wireless connection.

Select 'Access point', then click 'Next'.

☐ Enter settings for the wireless frequency and channels over which the device will operate, and indicate whether you wish to configure additional performance-enhancing settings:


Setup Wizard for P2P-LEFT.lcf
Configure WLAN
Edit physical WLAN settings
Select the frequency band and a radio channel for your first wireless network interface.
Please note that in some countries not all available channels may be used.
Frequency band:
2.4 GHz (802.11g/b/n)
Channel number:
Channel 11 (2.462 GHz)
Automatic Channel Selection works only for DFS enabled channels. To verify if you need to configure a fixed channel, please use the "show wlan" command on the CLI of the device. The target country has to be configured in advance for this.
Make further expert settings to increase the WLAN performance.

The specific antennas you plan to use will determine how to complete this dialog. Depending upon the capacity of your chosen antennas, complete the following settings:

– Frequency band: 2.4 GHz or 5 GHz

– Channel number: A list of available channels. When the frequency band is set to 5 GHz, this field is set to 'Automatic selection'.

– Make further explicit settings to increase the WLAN performance: Selecting this causes the Configure WLAN wizard to display additional configuration screens relating to hardware compression, QoS and IGMP snooping.

For the purpose of this example, the settings displayed (above) are used.

Click 'Next'.

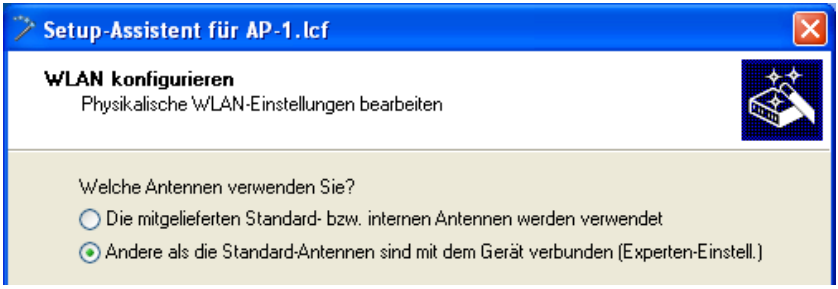
☐ The specific antennas you plan to use will determine how you complete this dialog. For the purpose of this example, enter the following settings:

– Frequency band: 2.4 GHz

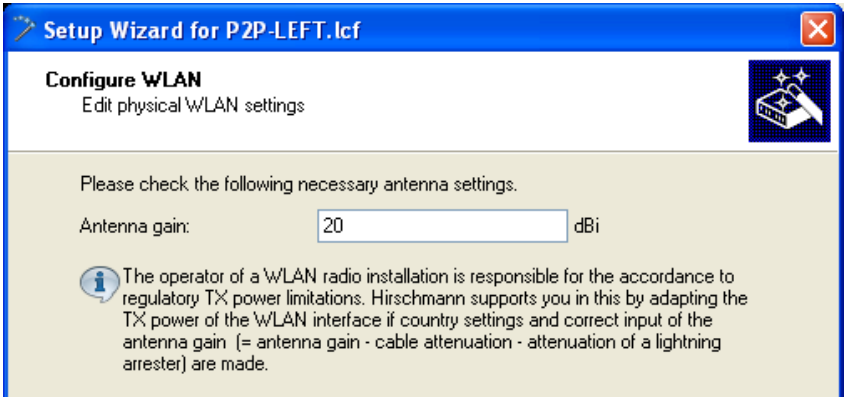
– Channel number: Channel 10 (2.457 GHz)

– Select 'Make further explicit settings to increase the WLAN performance'.
(This option gets the set-up wizard to display additional configuration screens for QoS and IGMP snooping.)

– Choose: 'Antennas other than the default antennas are connected to the device.'


Setup-Assistent für AP-1.lcf
WLAN konfigurieren
Physikalische WLAN-Einstellungen bearbeiten
Welche Antennen verwenden Sie?
Die mitgelieferten Standard- bzw. internen Antennen werden verwendet
Andere als die Standard-Antennen sind mit dem Gerät verbunden (Experten-Einstell.)

☐ If you elected to use 'Other than the default antennas...', specify how your antennas will be used:


Setup Wizard for P2P-LEFT.lcf
Configure WLAN
Edit physical WLAN settings
Please check the following necessary antenna settings.
Antenna gain:
20
dBi
The operator of a WLAN radio installation is responsible for the accordance to regulatory TX power limitations. Hirschmann supports you in this by adapting the TX power of the WLAN interface if country settings and correct input of the antenna gain (= antenna gain - cable attenuation - attenuation of a lightning arrester) are made.

How you configure this dialog depends on:

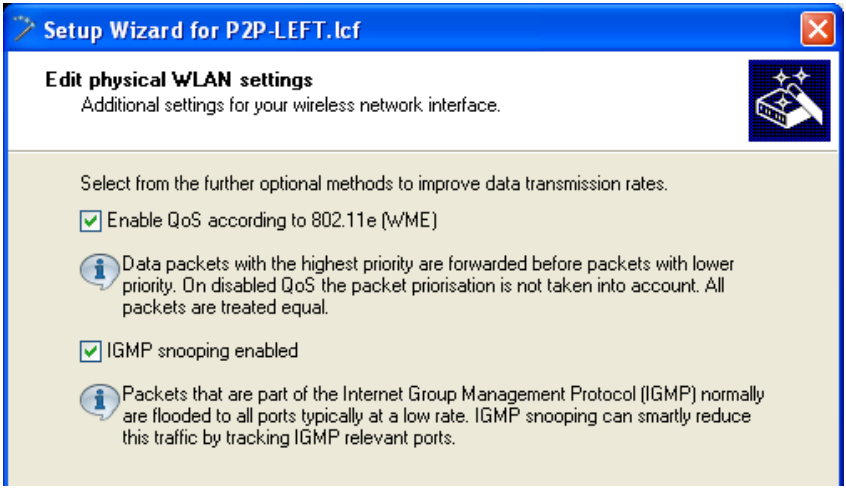
– the calculated antenna gain of the selected antennas

For the purpose of this example:

– antenna gain is 20 dBi

Click 'Next'.

☐ If you elected to 'Make further expert settings...', the wizard presents settings that can be used to increase data transmission rates:


Setup Wizard for P2P-LEFT.lcf
Edit physical WLAN settings
Additional settings for your wireless network interface.
Select from the further optional methods to improve data transmission rates.
Enable QoS according to 802.11e (WME)
Data packets with the highest priority are forwarded before packets with lower priority. On disabled QoS the packet priorisation is not taken into account. All packets are treated equal.
IGMP snooping enabled
Packets that are part of the Internet Group Management Protocol (IGMP) normally are flooded to all ports typically at a low rate. IGMP snooping can smartly reduce this traffic by tracking IGMP relevant ports.

You can enable or disable the following services:

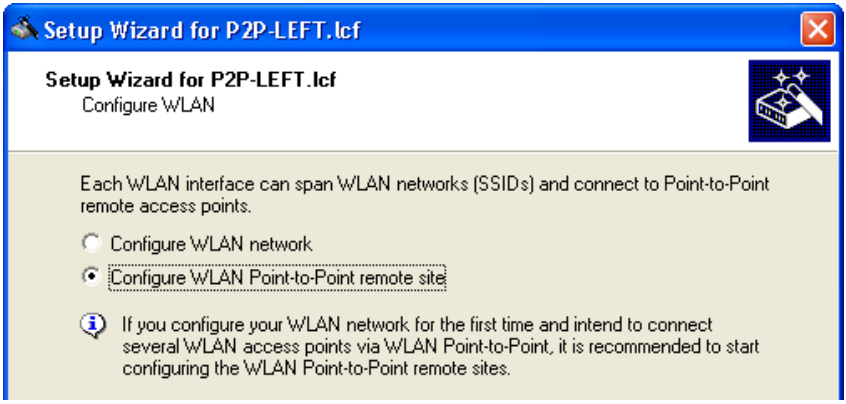
– QoS

– IGMP Snooping

For the purpose of this example, all available data rate enhancing options are selected.

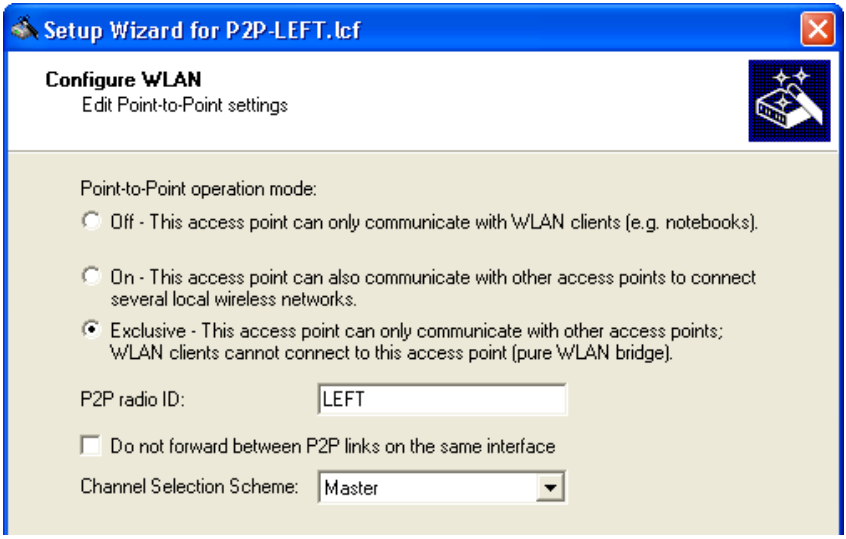
Click ‘Next’.

☐ Specify how this WLAN interface will be used:


Setup Wizard for P2P-LEFT.lcf
Setup Wizard for P2P-LEFT.lcf
Configure WLAN
Each WLAN interface can span WLAN networks (SSIDs) and connect to Point-to-Point remote access points.
Configure WLAN network
Configure WLAN Point-to-Point remote site
If you configure your WLAN network for the first time and intend to connect several WLAN access points via WLAN Point-to-Point, it is recommended to start configuring the WLAN Point-to-Point remote sites.

Select 'Configure WLAN Point-to-Point remote site', then click 'Next'.

☐ Specify the devices that will be permitted to communicate with this OpenBAT device:


Setup Wizard for P2P-LEFT.lcf
Configure WLAN
Edit Point-to-Point settings
Point-to-Point operation mode:
Off - This access point can only communicate with WLAN clients (e.g. notebooks).
On - This access point can also communicate with other access points to connect several local wireless networks.
Exclusive - This access point can only communicate with other access points; WLAN clients cannot connect to this access point (pure WLAN bridge).
P2P radio ID:
LEFT
Do not forward between P2P links on the same interface
Channel Selection Scheme:
Master

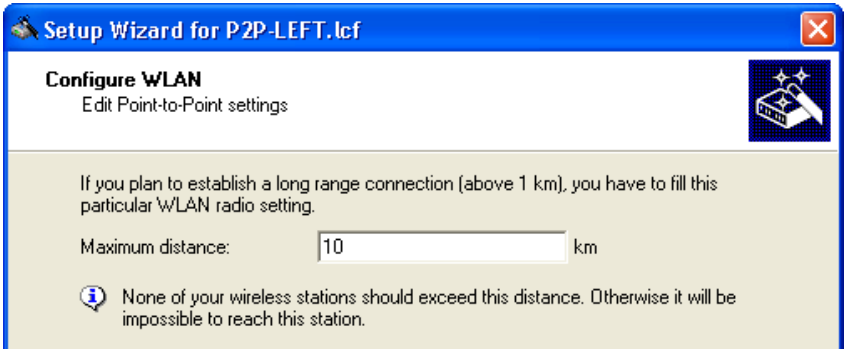
Configure the following configuration settings:

– Point-to-Point operation mode: determines which remote devices can wirelessly communicate with this WLAN device. The following options can be selected:
  - Off: only Clients
  - On: both Access Points and Clients
  - Exclusive: other Access Points exclusively
– P2P radio ID: a user-defined name for this OpenBAT device.
– Do not forward data between P2P connections of the same WLAN interface.
– Channel Selection Scheme: because both OpenBAT devices forming the point-to-point connection are Access Points, one needs to be configured as the master and one as the slave.

For the purpose of this example, the displayed settings (above) are selected.

Click ‘Next’.

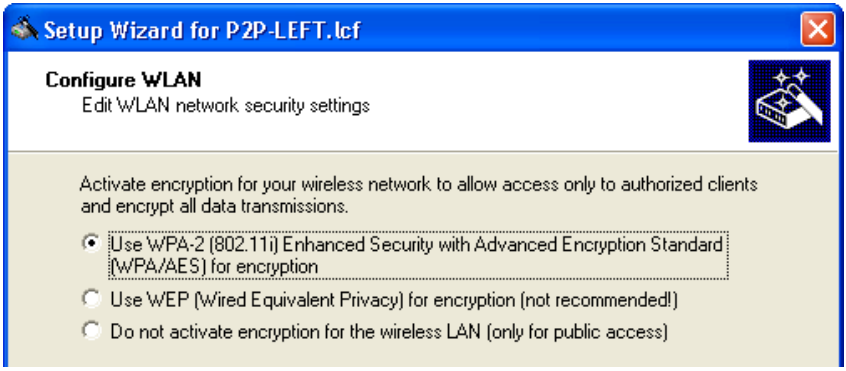
☐ Specify the maximum distance—in km—between the two access points forming the point-to-point WLAN bridge.


Setup Wizard for P2P-LEFT.lcf
Configure WLAN
Edit Point-to-Point settings
If you plan to establish a long range connection (above 1 km), you have to fill this particular WLAN radio setting.
Maximum distance:
10
km
None of your wireless stations should exceed this distance. Otherwise it will be impossible to reach this station.

In this example, a value of 10 km is used.

Click ‘Next’.

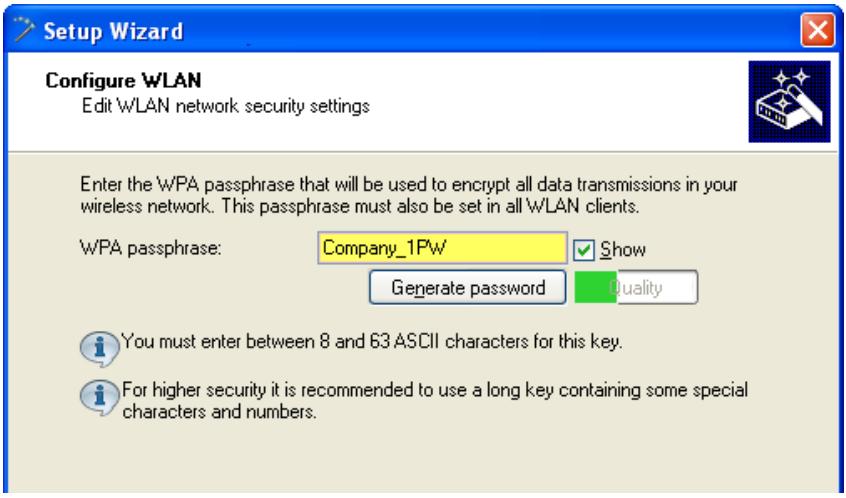
☐ Specify the transmission encryption protocol:


Setup Wizard for P2P-LEFT.lcf
Configure WLAN
Edit WLAN network security settings
Activate encryption for your wireless network to allow access only to authorized clients and encrypt all data transmissions.
Use WPA-2 (802.11i) Enhanced Security with Advanced Encryption Standard (WPA/AES) for encryption
Use WEP (Wired Equivalent Privacy) for encryption (not recommended!)
Do not activate encryption for the wireless LAN (only for public access)

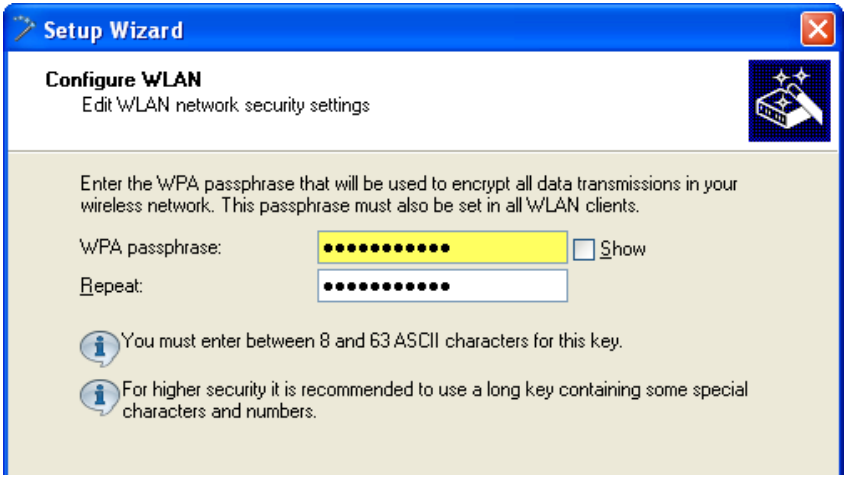
Note: Hirschmann recommends the use of WPA-2, to provide enhanced security.

Click ‘Next’.

- If you selected the WPA-2 encryption protocol, the following screen opens, where you enter a WPA passphrase—a string from 8 to 63 ASCII characters long—in one of the following ways:
  - Select ’Show’ (below), then do one of the following:
    - type in a new WPA passphrase
    - click ’Generate password’ and the wizard inputs a new string


Setup Wizard
Configure WLAN
Edit WLAN network security settings
Enter the WPA passphrase that will be used to encrypt all data transmissions in your wireless network. This passphrase must also be set in all WLAN clients.
WPA passphrase:
Company_1PW
Show
Generate password
Quality
You must enter between 8 and 63 ASCII characters for this key.
For higher security it is recommended to use a long key containing some special characters and numbers.

  - De-select ’Show’ (below) then type in a new WPA passphrase. In this case, you also re-type the password in the ’Repeat’ field:


Setup Wizard
Configure WLAN
Edit WLAN network security settings
Enter the WPA passphrase that will be used to encrypt all data transmissions in your wireless network. This passphrase must also be set in all WLAN clients.
WPA passphrase:
Show
Repeat:
You must enter between 8 and 63 ASCII characters for this key.
For higher security it is recommended to use a long key containing some special characters and numbers.

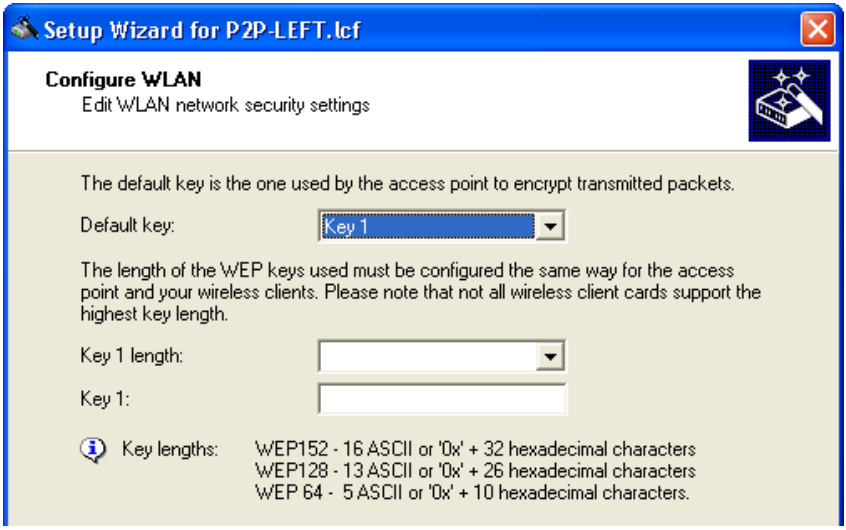
The role of the OpenBAT device in the point-to-point connection determines how the passphrase is used. If the device is configured as a:

– Master: the passphrase is used to check a slave's authorization to access the network.

– Slave: the passphrase is transferred to the Master to gain wireless access to the network.

In this example, type in the passphrase ’CompanyPW’, then click ’Next’.

▶ If you selected the WEP encryption protocol, the wizard prompts you to configure WEP keys:

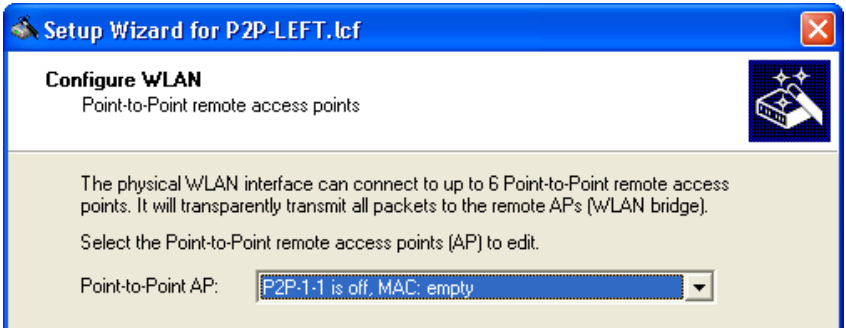

Setup Wizard for P2P-LEFT.lcf
Configure WLAN
Edit WLAN network security settings
The default key is the one used by the access point to encrypt transmitted packets.
Default key:
Key 1
The length of the WEP keys used must be configured the same way for the access point and your wireless clients. Please note that not all wireless client cards support the highest key length.
Key 1 length:
Key 1:
Key lengths:
WEP152 - 16 ASCII or '0x' + 32 hexadecimal characters
WEP128 - 13 ASCII or '0x' + 26 hexadecimal characters
WEP 64 - 5 ASCII or '0x' + 10 hexadecimal characters.

Use the WEP encryption configure the following settings:

– Default key: Select the key to be used for encrypting the packets sent by the access point. In this example, ‘Key 1’.
– Key 1 length: Select the key length to be used for the encryption of data packets on the WLAN. Please be aware that not every wireless card supports all key lengths.
– Key 1: Type in a passphrase value, for example, ‘private’.

Click ’Next’.

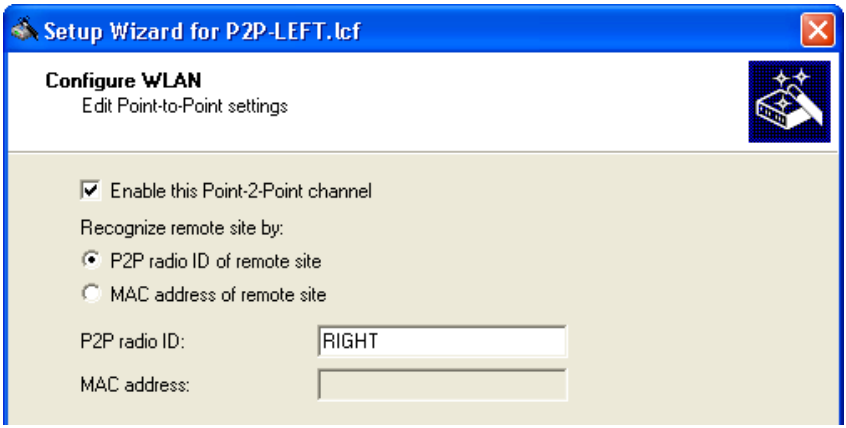
☐ Assign a point-to-point identifier to this WLAN interface:


Setup Wizard for P2P-LEFT.lcf
Configure WLAN
Point-to-Point remote access points
The physical WLAN interface can connect to up to 6 Point-to-Point remote access points. It will transparently transmit all packets to the remote APs (WLAN bridge).
Select the Point-to-Point remote access points (AP) to edit.
Point-to-Point AP:
P2P-1-1 is off, MAC: empty

Each OpenBAT device supports up to 6 point-to-point channels. Select an available point-to-point channel for this WLAN interface.

In this example, select the first available channel ('P2P-1-1'), then click 'Next'.

☐ Enable the assigned point-to-point channel:



Select the 'Enable the Point-2-Point channel' checkbox. Then indicate how to identify the remote access point at the other end of the point-to-point WLAN bridge, either by:

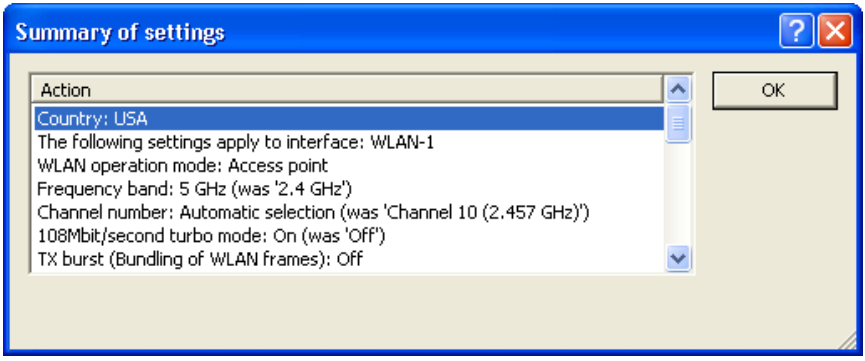
– its MAC Address
– a user-defined P2P radio identifier

In this example, use a user-defined P2P radio ID ('RIGHT'), then click 'Next'.

☐ You are now ready to complete the WLAN configuration.

Setup Wizard for P2P-LEFT.lcf
Setup Wizard for P2P-LEFT.lcf
You have successfully changed the WLAN settings.
Open the following table to get an overview of the changes made.
Summary of settings...
Select 'Finish' to apply the new settings.

Click on the 'Summary of settings... ' button to display a list of all the settings for this device.


Summary of settings
Action
OK
Country: USA
The following settings apply to interface: WLAN-1
WLAN operation mode: Access point
Frequency band: 5 GHz (was '2.4 GHz')
Channel number: Automatic selection (was 'Channel 10 (2.457 GHz)')
108Mbit/second turbo mode: On (was 'Off')
TX burst (Bundling of WLAN frames): Off

Click 'OK' to close the summary.

Click 'Finish' to close the wizard and save your settings.

3.5.2 Configuring the RIGHT Device

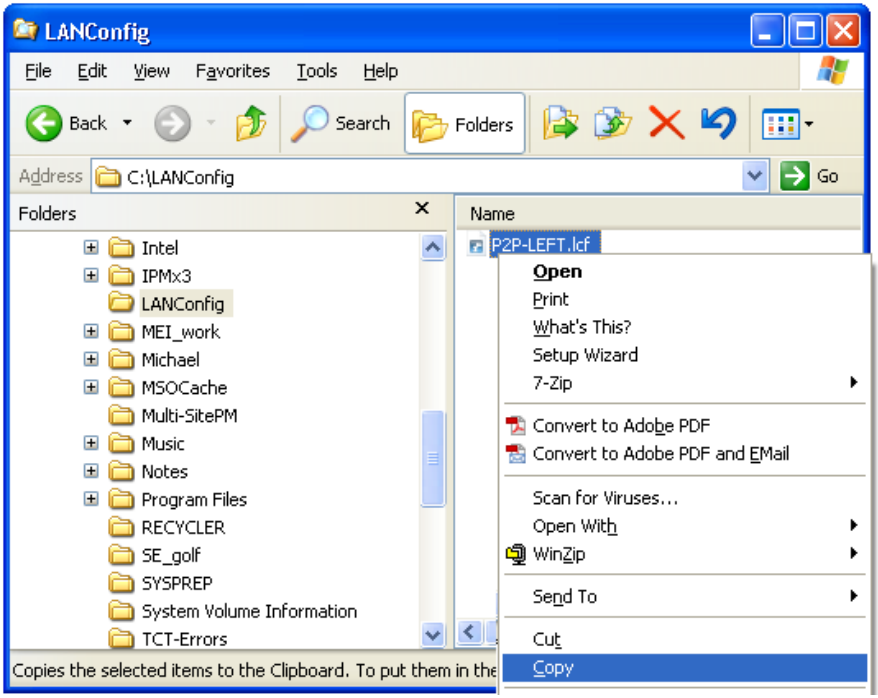
Both the LEFT and RIGHT OpenBAT devices are of the same device type equipped with the same firmware version. Consequently, the quickest way to create a configuration file for the RIGHT device is to copy the configuration file of the LEFT device and edit a few settings.

Creating a New Configuration File

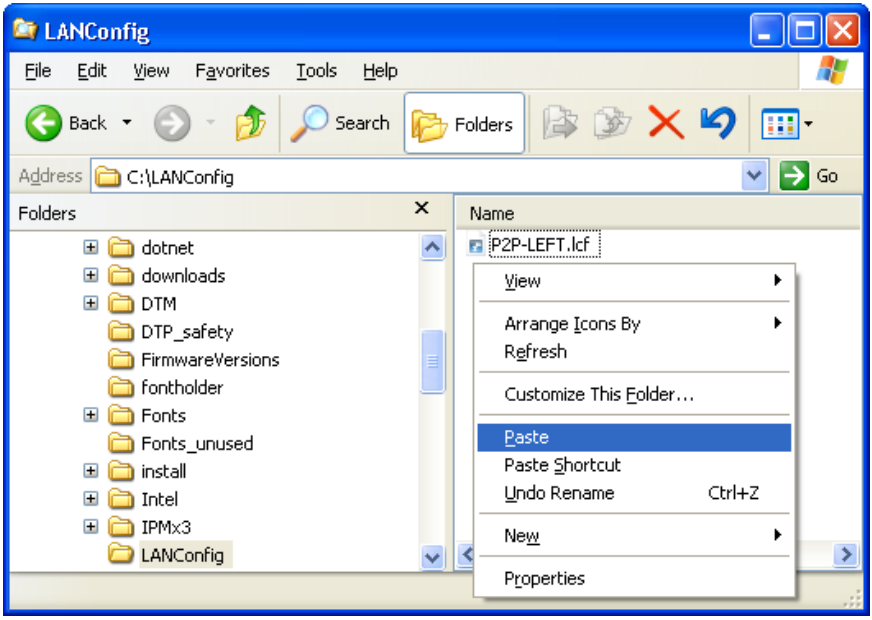
To begin the process of configuring the RIGHT device, locate the LANconfig file for the LEFT device on your PC's hard drive.

☐ Open Windows Explorer and navigate to the folder containing the LANconfig file `P2P-LEFT.lcf`.

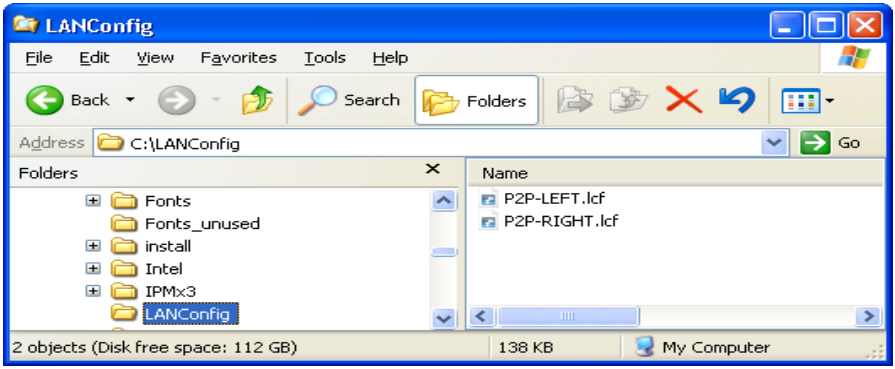
☐ Copy the LANconfig file `P2P-LEFT.lcf`:



☐ Paste the copied file into the same folder in Windows Explorer.

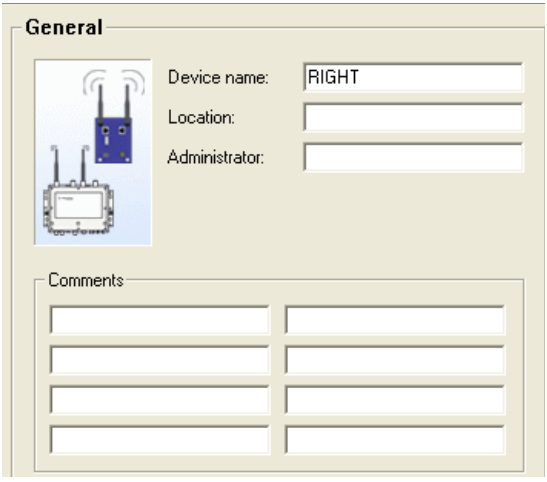


☐ Rename the copied file to `P2P-RIGHT.lcf`.



☐ Select the `P2P-RIGHT.lcf` file in Windows Explorer, then double-click the left mouse button. The LANconfig software opens for editing the RIGHT device configuration file.

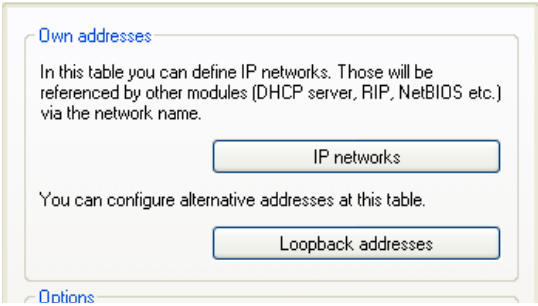
☐ Open the `Configuration : Management : General`.



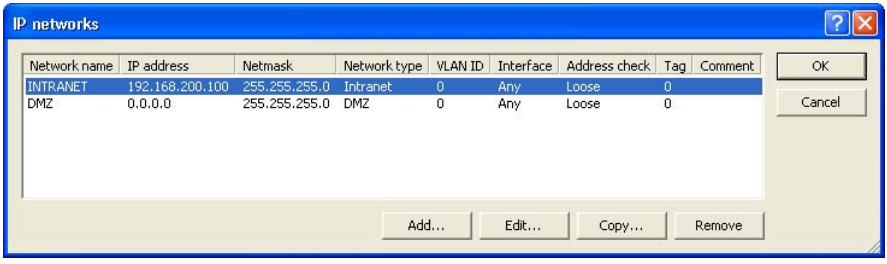
Type in ’RIGHT’ as the new ’Device name’.

☐ Edit the device IP address. To do this, navigate through several software screens, as follows:

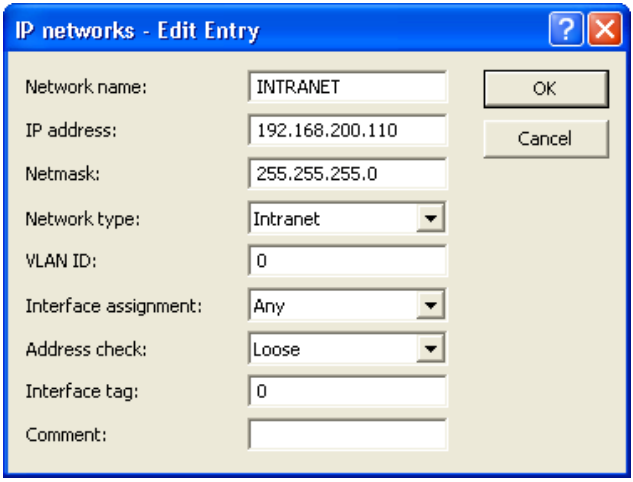
☐ Open the `Configuration : IPv4 : General` dialog.


Own addresses
In this table you can define IP networks. Those will be referenced by other modules (DHCP server, RIP, NetBIOS etc.) via the network name.
IP networks
You can configure alternative addresses at this table.
Loopback addresses
Options

☐ Click on the 'IP networks...' button (above) to open the 'IP networks' window (below):



☐ Click on the 'Edit...' button (above) to open the 'Edit Entry' dialog (below):



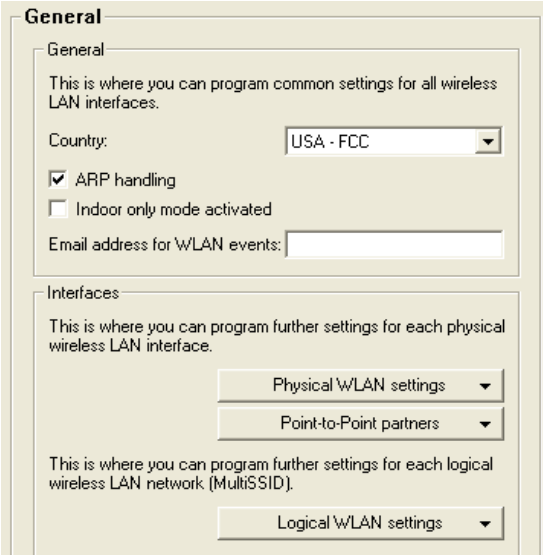
In the ‘Edit Entry’ dialog change the IP address to 192.168.200.110.

Click ’OK’ to close the ‘Edit Entry’ dialog.

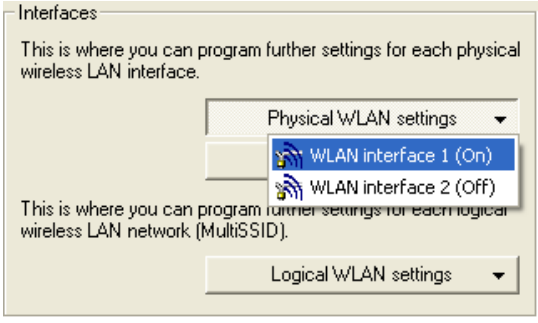
Click ’OK’ a second time to close the ‘IP networks’ dialog and return to the `Configuration : IPv4 : General` dialog.

☐ Edit the station name and channel selection scheme for this OpenBAT device. In this case, the station name is 'RIGHT' and the channel selection scheme is 'Slave'. As before, navigate through the following software screens:

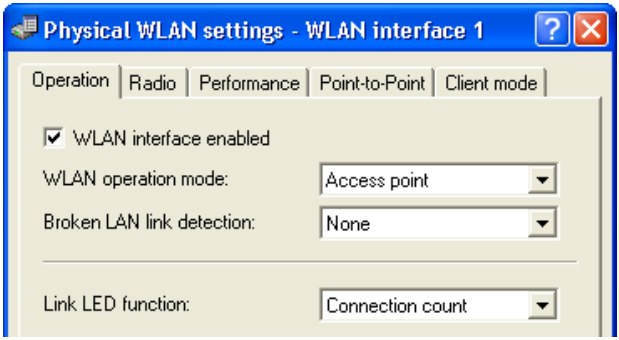
☐ Open the `Configuration : Wireless LAN : General` dialog:


General
General
This is where you can program common settings for all wireless LAN interfaces.
Country:
USA - FCC
ARP handling
Indoor only mode activated
Email address for WLAN events:
Interfaces
This is where you can program further settings for each physical wireless LAN interface.
Physical WLAN settings
Point-to-Point partners
This is where you can program further settings for each logical wireless LAN network (MultiSSID).
Logical WLAN settings

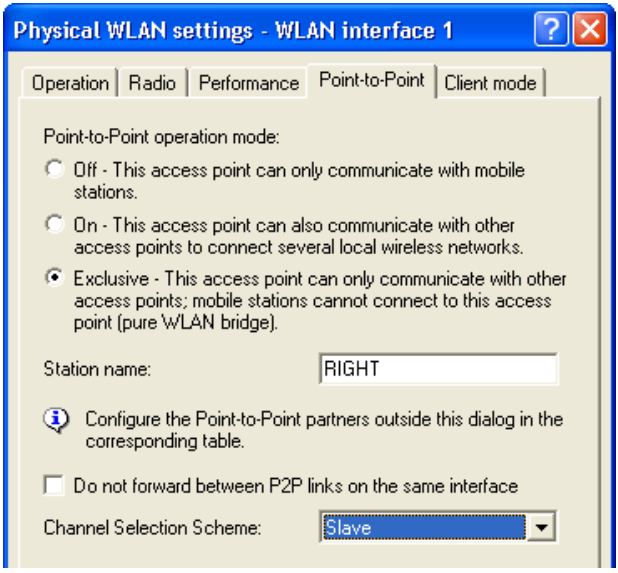
☐ Click on the 'Physical WLAN settings' button (above). If your device has two WLAN interfaces, select 'WLAN interface 1':


Interfaces
This is where you can program further settings for each physical wireless LAN interface.
Physical WLAN settings
WLAN interface 1 (On)
WLAN interface 2 (Off)
wireless LAN network (MultiSSID).
Logical WLAN settings

A dialog for editing the physical WLAN settings of WLAN interface 1 opens:



☐ Select the 'Point-to-Point' tab (above) to display a dialog for where you can configure point-to-point operation settings (below):


Physical WLAN settings - WLAN interface 1
Operation
Radio
Performance
Point-to-Point
Client mode
Point-to-Point operation mode:
Off - This access point can only communicate with mobile stations.
On - This access point can also communicate with other access points to connect several local wireless networks.
Exclusive - This access point can only communicate with other access points; mobile stations cannot connect to this access point (pure WLAN bridge).
Station name:
RIGHT
Configure the Point-to-Point partners outside this dialog in the corresponding table.
Do not forward between P2P links on the same interface
Channel Selection Scheme:
Slave

Make the following edits:.

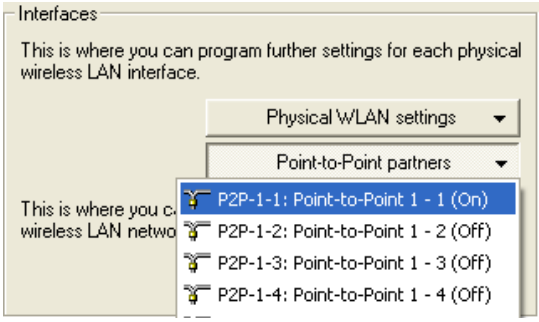
- Station name: 'RIGHT'

-Channel Selection Scheme: 'Slave'

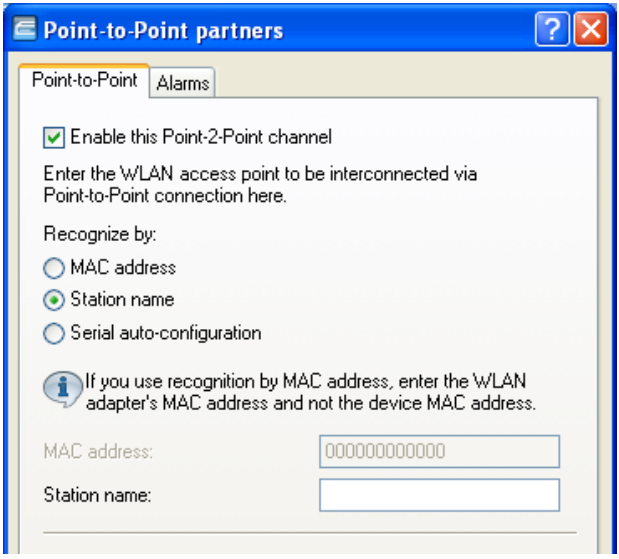
Click 'Next'.

☐ The final edit is to change the station name of the point-to-point partner. In this case, the partner is the 'LEFT' device. Navigate to the screen where you can make this edit, as follows:

  ☐ In the Wireless LAN configuration dialog, click on the 'Point-to-Point partners' button, and select 'P2P-1-1' (below):


Interfaces
This is where you can program further settings for each physical wireless LAN interface.
Physical WLAN settings
Point-to-Point partners
This is where you c
wireless LAN netwo
P2P-1-1: Point-to-Point 1 - 1 (On)
P2P-1-2: Point-to-Point 1 - 2 (Off)
P2P-1-3: Point-to-Point 1 - 3 (Off)
P2P-1-4: Point-to-Point 1 - 4 (Off)

☐ The next dialog for editing the Point-to-Point channels opens:


Point-to-Point partners
Point-to-Point
Alarms
Enable this Point-2-Point channel
Enter the WLAN access point to be interconnected via Point-to-Point connection here.
Recognize by:
MAC address
Station name
Serial auto-configuration
If you use recognition by MAC address, enter the WLAN adapter's MAC address and not the device MAC address.
MAC address:
000000000000
Station name:

Change the partner ’Station name’ to ’LEFT’.

Click ’OK’ to close the dialog.

Click ’OK’ again to close the file and save your edits.

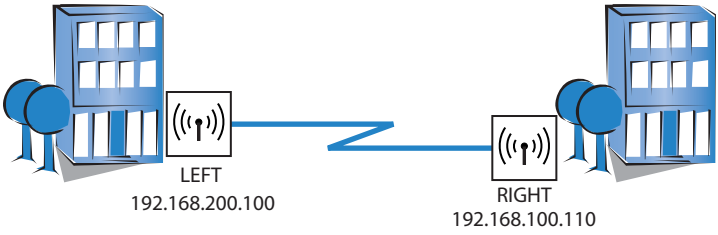
3.6 WLAN Bridge: Two Subnets

This example shows the creation of a WLAN bridge between 2 OpenBAT devices that are situated in different subnets by:

- ☐ creating a dedicated transfer network connecting the two OpenBAT devices, then
- ☐ routing the data traffic from one subnet to the other over the newly created transfer network

The transfer network's single purpose is to connect the two OpenBAT devices and thereby establishing a connection between the two subnets.

As before, each Access Point is configured to deny access to devices other than its bridge partner. This example builds on the previous configurations of the RIGHT and LEFT devices (see on page 105) and enables routing between these two devices.



The significant configuration settings for the device are as follows:

Station Name:	LEFT	RIGHT
Role:	Access Point	Access Point
IP address:	192,168,200,100	192,168,100,110
Subnet Mask:	255.255.255.0	255.255.255.0
Channel Selection Scheme	Master	Slave
Point-to-Point Partner	RIGHT	LEFT

3.6.1 Creating Two LANconfig Files

Creating a WLAN bridge between two different subnets involves the creation and configuration of two LANconfig files, one for the LEFT device and one for the RIGHT device. Because these two files contain virtually the same Basic settings (see on page 106) and WLAN settings (see on page 114) as in the previous example, the easiest way to begin is to copy and re-name previously created files. After new files are created, their configuration settings can be edited.

To create two LANconfig files, follow these steps:

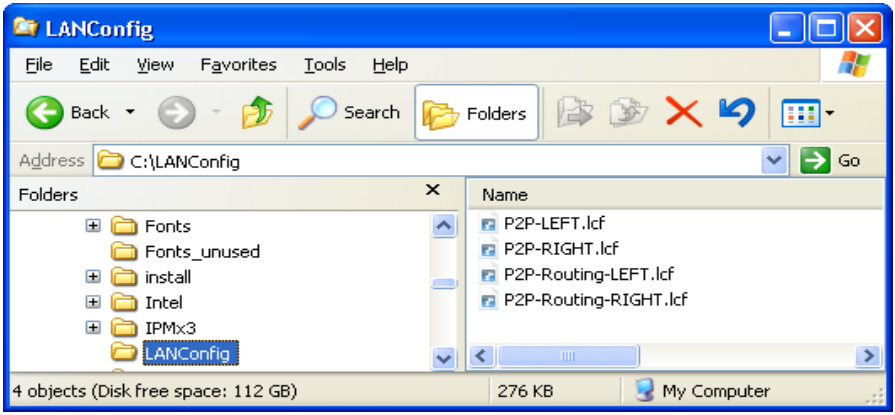
☐ Create a new LANconfig file: `P2P-Routing-LEFT.lcf`:

- In Windows Explorer, navigate to the folder where the previously created LANconfig files are saved.
- Copy the file `P2P-LEFT.lcf`.
- Paste the copied file into the same Windows Explorer folder.
- Rename the new file `P2P-Routing-LEFT.lcf`.

☐ Create a new LANconfig file: `P2P-Routing-RIGHT.lcf`.

- In Windows Explorer, navigate to the folder where the previously created LANconfig files are saved.
- Copy the file `P2P-RIGHT.lcf`.
- Paste the copied file into the same Windows Explorer folder.
- Rename the new file `P2P-Routing-RIGHT.lcf`.

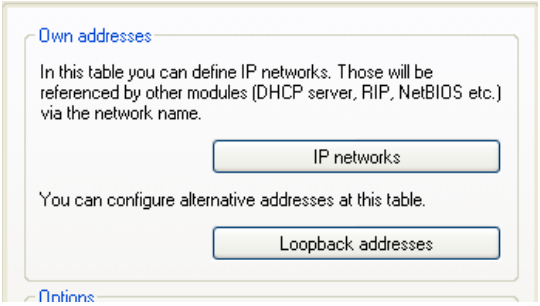
Windows Explorer now contains the following files:



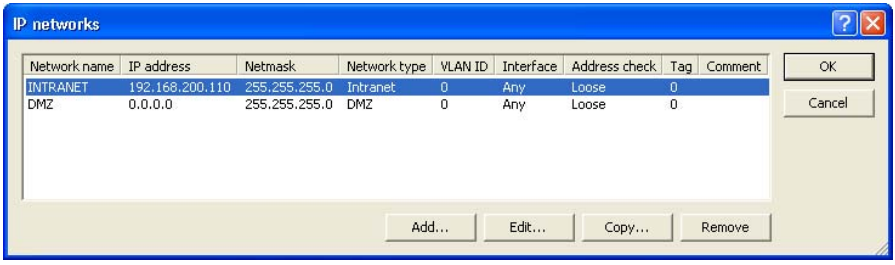
☐ The next step is to edit the IP address of the RIGHT device:

☐ In Windows Explorer, double-click on the file: `P2P-Routing-RIGHT.lcf`.

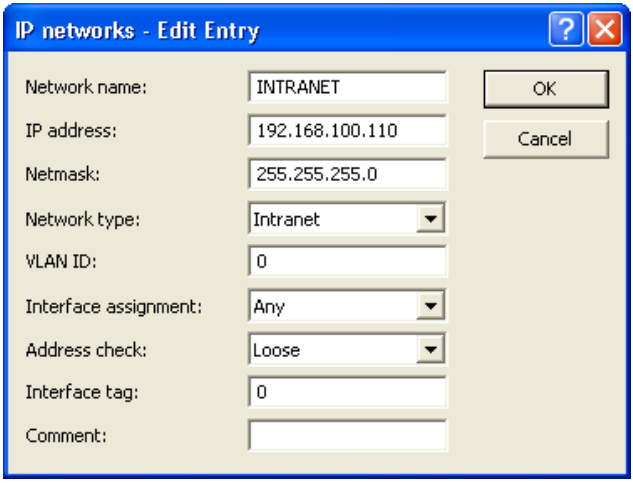
☐ Open the `Configuration : IPv4 : General` dialog.


Own addresses
In this table you can define IP networks. Those will be referenced by other modules (DHCP server, RIP, NetBIOS etc.) via the network name.
IP networks
You can configure alternative addresses at this table.
Loopback addresses
Options

☐ Click the 'IP networks...: button (above) to open the 'IP networks' window (below):



☐ In the ‘IP networks’ window (above) select the INTRANET network, then click on the ’Edit...’ button to open the ‘Edit Entry’ dialog (below):



☐ In the ‘Edit Entry’ dialog, edit the IP address of the RIGHT device configuration file to 192.168.100.110.

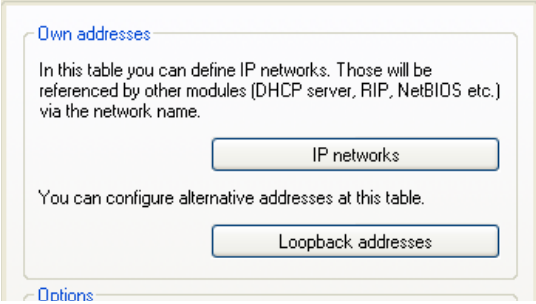
☐ Click ’OK’ three times to close the open dialogs, save your edits and close the file `P2P-Router-RIGHT.lcf`.

3.6.2 Creating Two Transfer Network Entries

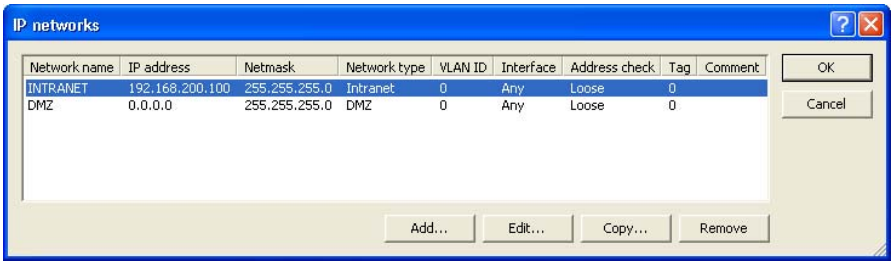
The next task is to create a transfer network in each device. This is accomplished by adding a new network entry to each device configuration file.

☐ In Windows Explorer, click on the file `P2P-Routing-LEFT.lcf` to open it for editing.

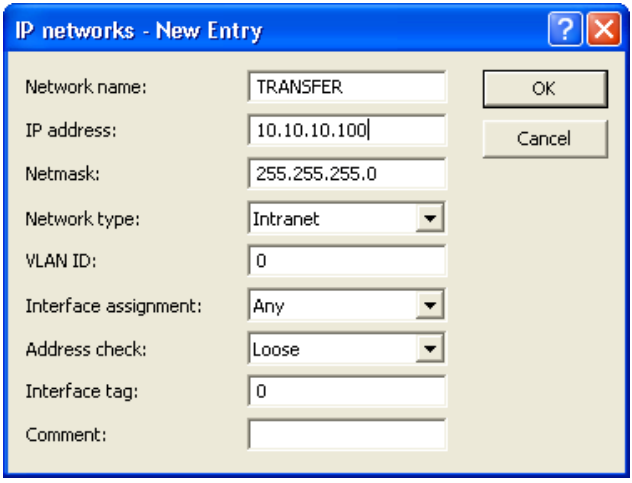
☐ Open the `Configuration : IPv4 : General` dialog.


Own addresses
In this table you can define IP networks. Those will be referenced by other modules (DHCP server, RIP, NetBIOS etc.) via the network name.
IP networks
You can configure alternative addresses at this table.
Loopback addresses
Options

☐ Click the 'IP networks...: button (above) to open the 'IP networks' window (below):



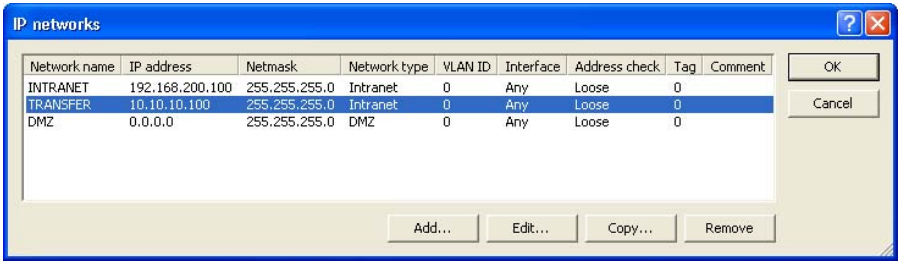
☐ In the 'IP networks' window (above), click the 'Add...' button to open the 'New Entry' dialog (below):



☐ In the ‘New Entry’ dialog (above), create a new network for this device configuration file by inputting the following settings:

- Network name: TRANSFER
- IP address: 10.10.10.100
- Network type: Intranet (the default)
- VLAN ID: 0 (the default)
- Interface assignment: Any (the default)
- Address check: Loose (the default)
- Interface tag: 0 (the default)
- Comment: <leave blank>

Click ’OK’ to add the new network to the network list in the ‘IP networks’ window (below):



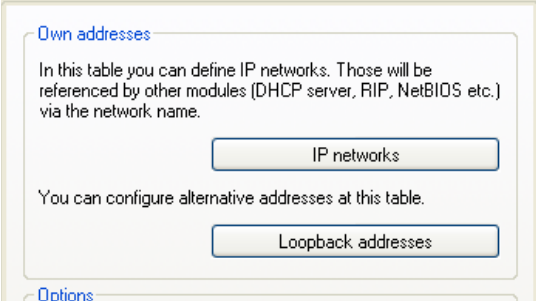
☐ Click ’OK’ again to close the ‘IP networks’ window for the LEFT device.

Note: Leave open the `P2P-Routing-LEFT.lcf` LANconfig file for further editing.

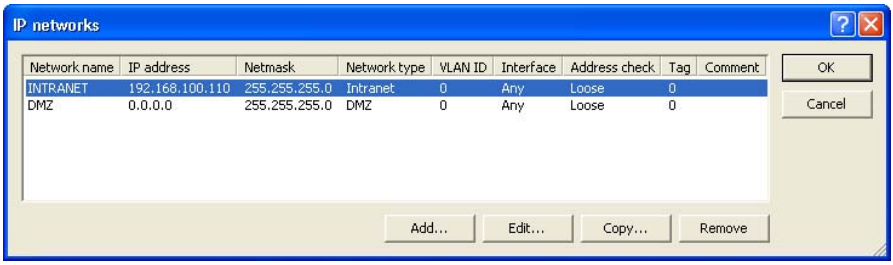
The next step is to create a new network entry for the RIGHT device, as described, below.

☐ In Windows Explorer, click on the file `P2P-Routing-RIGHT.lcf` to open it for editing.

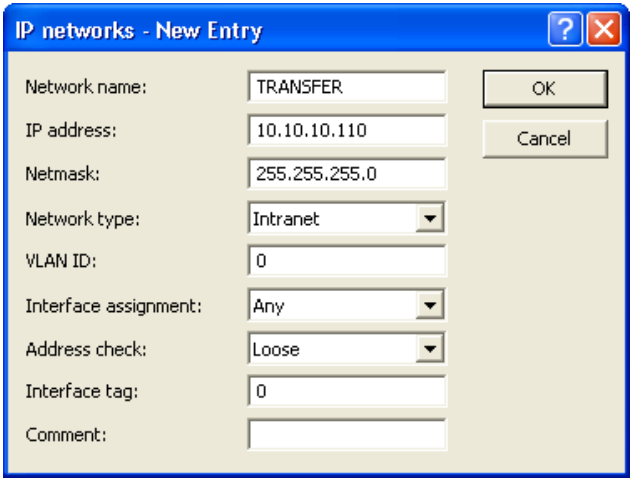
☐ Open the `Configuration : IPv4 : General dialog.`


Own addresses
In this table you can define IP networks. Those will be referenced by other modules (DHCP server, RIP, NetBIOS etc.) via the network name.
IP networks
You can configure alternative addresses at this table.
Loopback addresses
Options

☐ Click on the 'IP networks...' button (above) to open the 'IP networks' window (below):



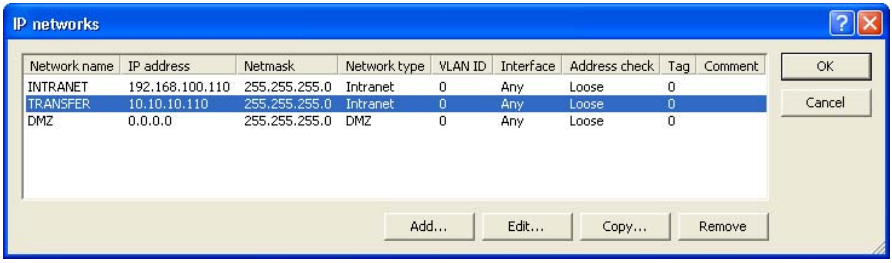
☐ In the 'IP networks' window (above), click the 'Add...' button to open the 'New Entry' dialog (below):



☐ In the ‘New Entry’ dialog (above), create a new network for this device configuration file by inputting the following settings:

- Network name: TRANSFER
- IP address: 10.10.10.110
- Network type: Intranet (the default)
- VLAN ID: 0 (the default)
- Interface assignment: Any (the default)
- Address check: Loose (the default)
- Interface tag: 0 (the default)
- Comment: <leave blank>

Click ’OK’ to add the new network to the network list in the ‘IP networks’ window (below):



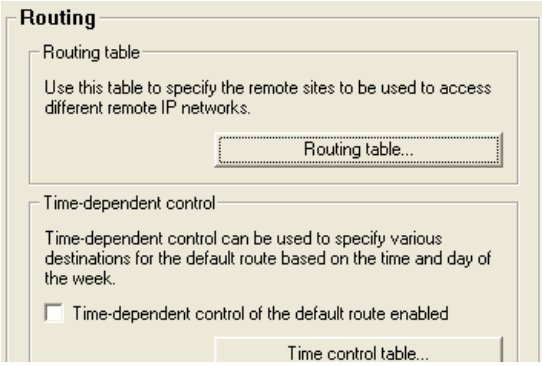
☐ Click ’OK’ again to close the ‘IP networks’ window for the RIGHT device.

Note: Leave open the `P2P-Routing-RIGHT.lcf` LANconfig file for further editing.

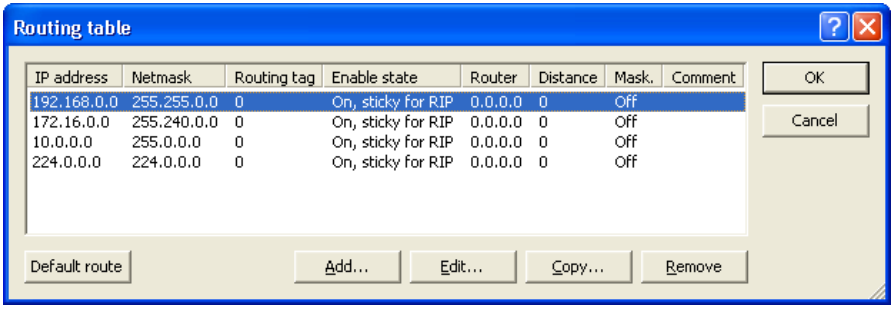
3.6.3 Routing the Transfer Networks

The next step is to link together the two new transfer networks. This is accomplished by assigning each new network to the same routing address.

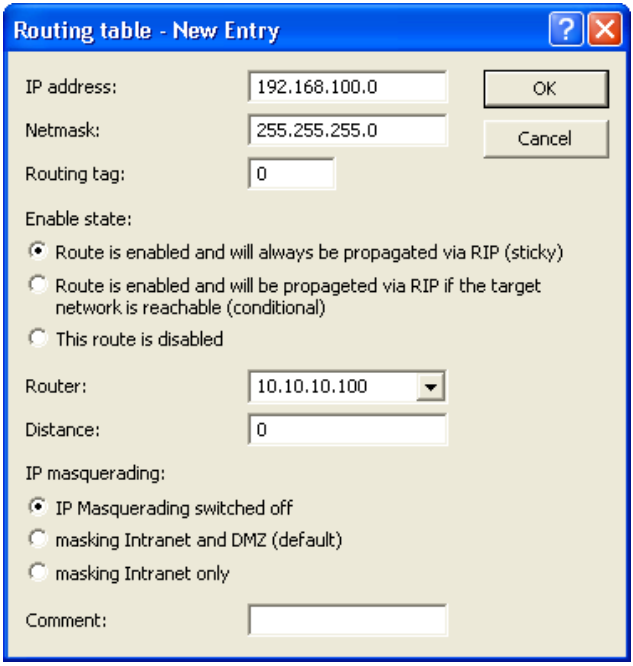
☐ Return to the configuration file `P2P-Routing-LEFT.lcf` (which remains open) and open the `Configuration : IP Router : Routing` dialog:


Routing
Routing table
Use this table to specify the remote sites to be used to access different remote IP networks.
Routing table...
Time-dependent control
Time-dependent control can be used to specify various destinations for the default route based on the time and day of the week.
Time-dependent control of the default route enabled
Time control table...

☐ Click on the 'Routing table...' button (above) to open the routing table for the LEFT device (below):


Routing table
IP address Netmask Routing tag Enable state Router Distance Mask. Comment
192.168.0.0 255.255.0.0 0 On, sticky for RIP 0.0.0.0 0 Off
172.16.0.0 255.240.0.0 0 On, sticky for RIP 0.0.0.0 0 Off
10.0.0.0 255.0.0.0 0 On, sticky for RIP 0.0.0.0 0 Off
224.0.0.0 224.0.0.0 0 On, sticky for RIP 0.0.0.0 0 Off
OK
Cancel
Default route
Add...
Edit...
Copy...
Remove

☐ In the 'Routing table' (above), click on the 'Add...: button to open the 'New Entry' dialog (below):

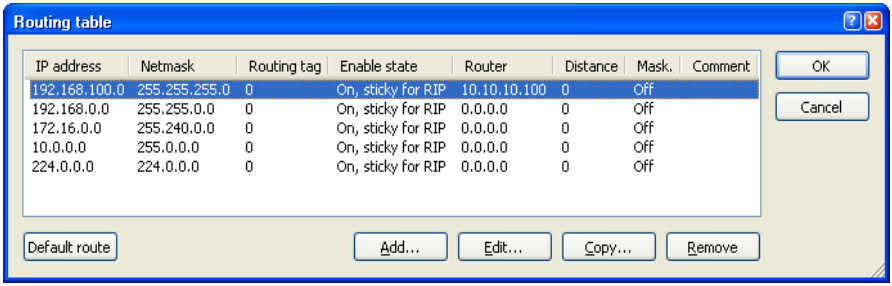


☐ In the ‘New Entry’ dialog (above), create a new routing entry and associate that routing entry with the network of the RIGHT device, as follows:

– IP address: 192.168.100.0
– Netmask: 255.255.255.0
– Router: 10.10.10.100

Accept the remaining default values.

Click ’OK’ to save the new routing entry, and add it to the Routing table (below):



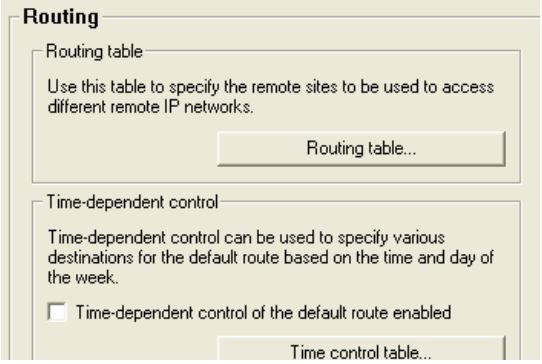
☐ Click 'OK' to close the routing table (above) for the LEFT device.

Click 'OK' a second time to save both the new network and the routing settings for the `P2P-Routing-LEFT.lcf` configuration file.

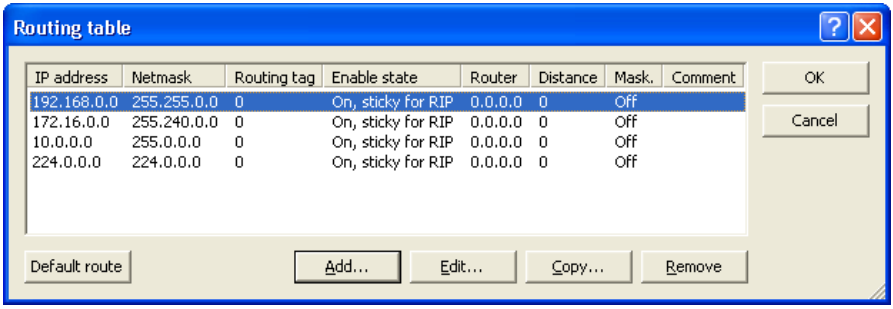
The next task is to create a new routing table entry for the RIGHT device.

☐ Return to the configuration file `P2P-Routing-RIGHT.lcf` (which remains open).

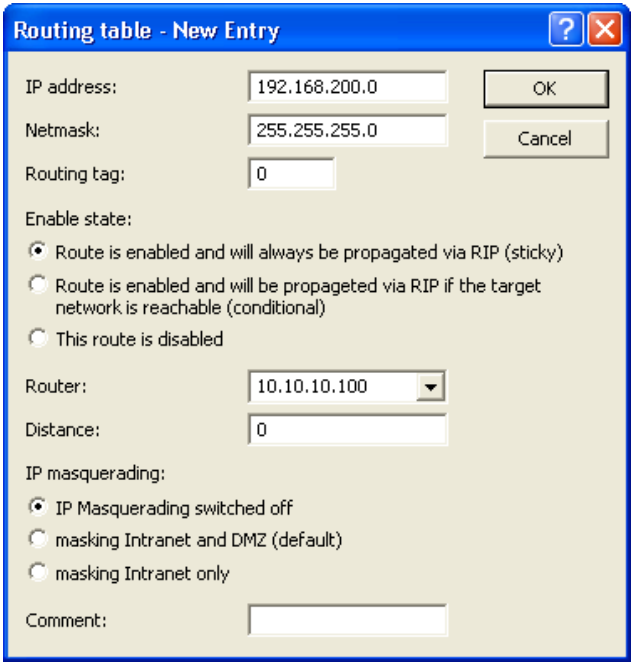
☐ Open the `Configuration : IP Router : Routing` dialog:


Routing
Routing table
Use this table to specify the remote sites to be used to access different remote IP networks.
Routing table...
Time-dependent control
Time-dependent control can be used to specify various destinations for the default route based on the time and day of the week.
Time-dependent control of the default route enabled
Time control table...

☐ Click on the 'Routing table...' button (above) to open the routing table for the RIGHT device (below):



☐ In the ‘Routing table’ (above), click on the ’Add...: button to open the ‘New Entry’ dialog (below):

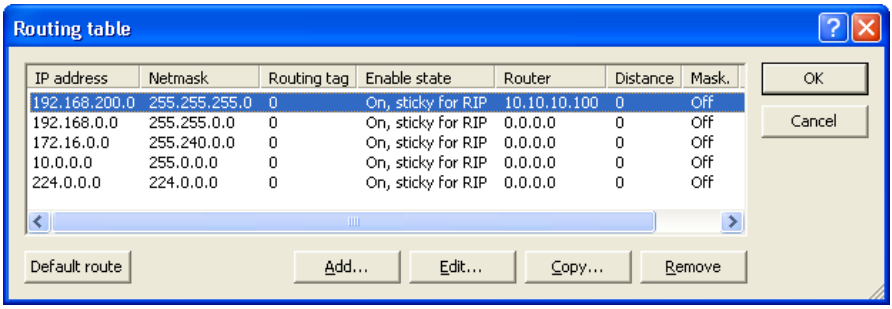


☐ In the ‘New Entry’ dialog (above), create a new routing entry and associate that routing entry with the network of the LEFT device, as follows:

– IP address: 192.168.200.0
– Netmask: 255.255.255.0
– Router: 10.10.10.100

Accept the remaining default values.

Click ’OK’ to save the new routing entry, and add it to the Routing table (below):



☐ Click ’OK’ to close the routing table (above) for the RIGHT device.

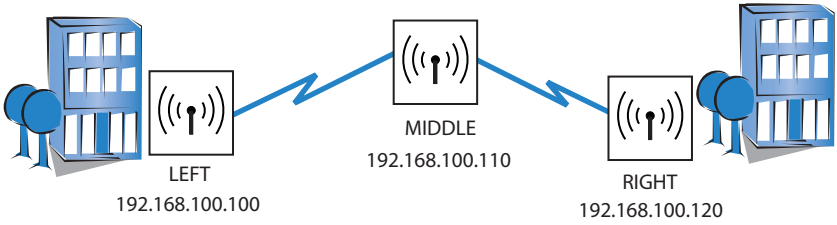
Click ’OK’ a second time to save both the new network and the routing settings for the `P2P-Routing-RIGHTT.lcf` configuration file.

Configurations for the transfer network are complete.

3.7 WLAN Bridge Relay: 1 Radio

This example employs three OpenBAT devices (named LEFT, CENTER, and RIGHT) to implement a WLAN bridge relay. All devices are located in the same subnet.

The CENTER device serves as a repeater and relays messages between the LEFT and RIGHT devices. The CENTER device communicates with both the LEFT and RIGHT devices via two different channels over a single radio interface. Because the relay device employs just a single radio, this design reduces the effective bandwidth of the connection by a factor of 50%.



The significant configuration settings for the device are as follows:

Station Name:	LEFT	CENTER	RIGHT
Role:	Access Point	Access Point	Access Point
IP address:	192,168,100,100	192,168,100,110	192,168,100,120
Subnet Mask:	255.255.255.0	255.255.255.0	255.255.255.0
Number of interfaces used:	1	1	1
Number of channels used:	1	2	1
Channel Selection Scheme	Slave	Master	Slave
Point-to-Point Partner	CENTER	LEFT/RIGHT	CENTER

Each Access Point is configured to deny access to devices other than its immediate bridge partner. This example builds on the previous configurations of the LEFT and RIGHT devices (see on page 105).

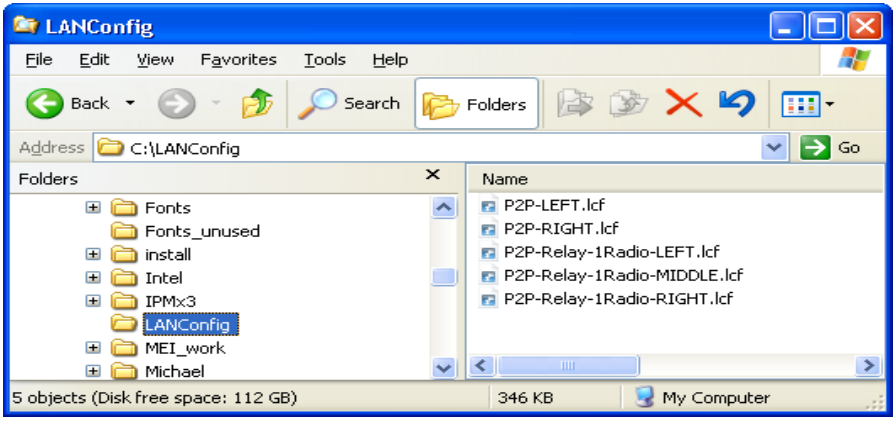
3.7.1 Creating Three LANconfig Files

Creating a WLAN bridge relay involves the creation and configuration of three LANconfig files, one for the LEFT device, one for the MIDDLE device, and one for the RIGHT device. Because each of these files contain virtually the same Basic settings (see on page 106) and WLAN settings (see on page 114) as in the original example, the easiest way to begin is to make 3 copies of the previously `P2P-LEFT.lcf` file. After new files are created, their configuration settings can be edited.

To create three new LANconfig files, follow these steps:

- ☐ Create a new LANconfig file: `P2P-Relay-1Radio-LEFT.lcf`:
  - ☐ In Windows Explorer, navigate to the folder where the previously created LANconfig files are saved.
  - ☐ Copy the file `P2P-LEFT.lcf`.
  - ☐ Paste the copied file into the same Windows Explorer folder.
  - ☐ Rename the new file `P2P-Relay-1Radio-LEFT.lcf`.
- ☐ Create a new LANconfig file: `P2P-Relay-1Radio-MIDDLE.lcf`:
  - ☐ In Windows Explorer, navigate to the folder where the previously created LANconfig files are saved.
  - ☐ Copy the file `P2P-LEFT.lcf`.
  - ☐ Paste the copied file into the same Windows Explorer folder.
  - ☐ Rename the new file `P2P-Relay-1Radio-MIDDLE.lcf`.
- ☐ Create a new LANconfig file: `P2P-Relay-1Radio-RIGHT.lcf`.
  - ☐ In Windows Explorer, navigate to the folder where the previously created LANconfig files are saved.
  - ☐ Copy the file `P2P-LEFT.lcf`.
  - ☐ Paste the copied file into the same Windows Explorer folder.
  - ☐ Rename the new file `P2P-Relay-1Radio-RIGHT.lcf`.

  Windows Explorer now contains the following files:



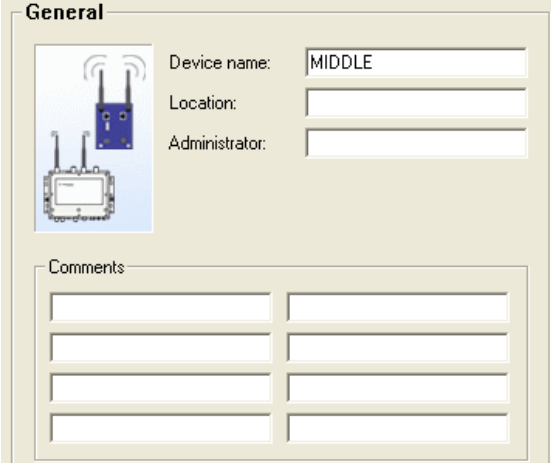
The next tasks are to edit the names and IP addresses of both the MIDDLE and RIGHT devices.

Note: The file `P2P-Relay-1Radio-LEFT.lcf` should be configured with the:
- Device name = 'LEFT', and
- IP address = '192.168.100.100'

☐ To edit the name and IP address of the MIDDLE device:

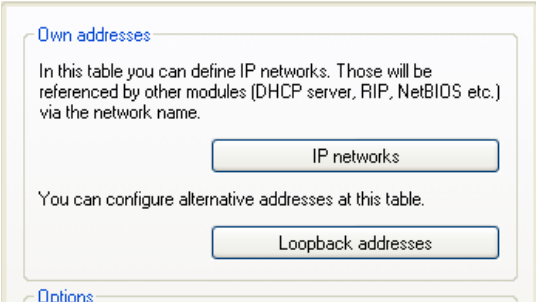
☐ In Windows Explorer, double-click on the file: `P2P-Relay-1Radio-MIDDLE.lcf`.

☐ Open the `Configuration : Management : General` dialog.

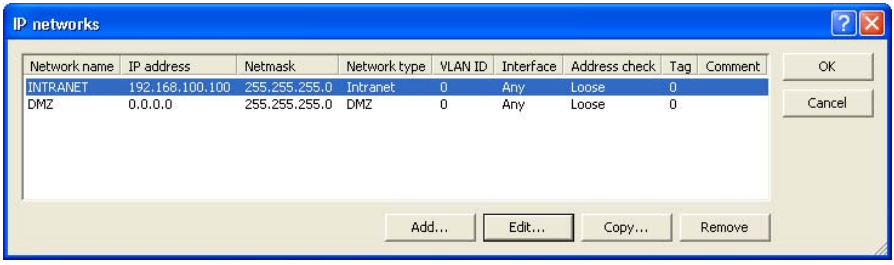


☐ Change the Device name to 'MIDDLE'.

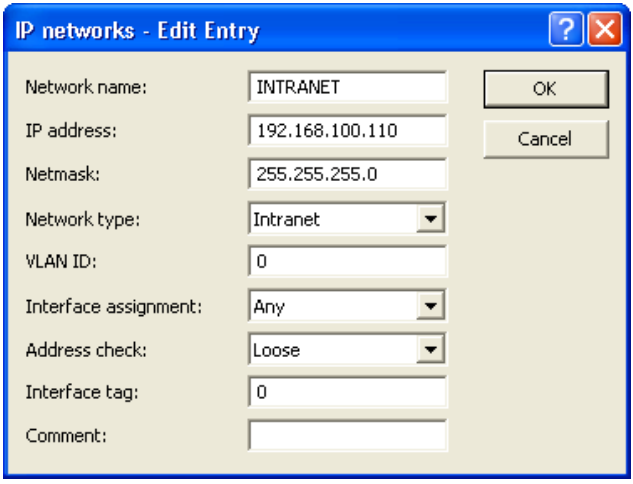
☐ Open the `Configuration : IPv4 : General` dialog.


Own addresses
In this table you can define IP networks. Those will be referenced by other modules (DHCP server, RIP, NetBIOS etc.) via the network name.
IP networks
You can configure alternative addresses at this table.
Loopback addresses
Options

☐ Click the 'IP networks...' button (above) to open the 'IP networks' window (below):



☐ In the ‘IP networks’ window (above), select the INTRANET network, then click the ’Edit...’ button to open the ‘Edit Entry’ dialog (below):



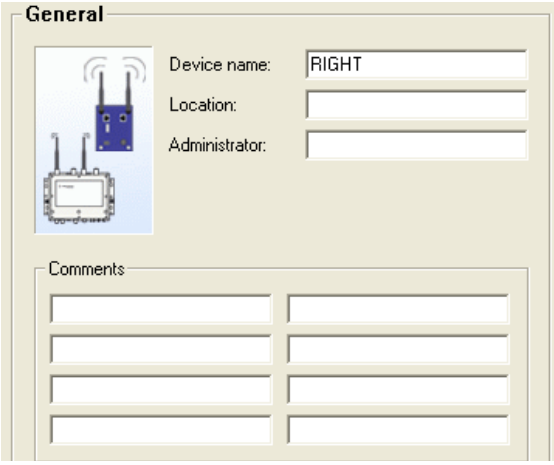
☐ In the ‘Edit Entry’ dialog, change the IP address of the MIDDLE device configuration file to ’192.168.100.110’.

☐ Click ’OK’ twice. Leave the configuration file open for later editing.

☐ To edit the name and IP address of the RIGHT device:

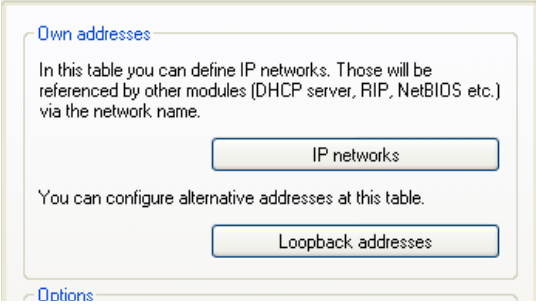
☐ In Windows Explorer, double-click on the file:
`P2P-Relay-1Radio-RIGHT.lcf`.

☐ Open the `Configuration : Management : General` dialog:

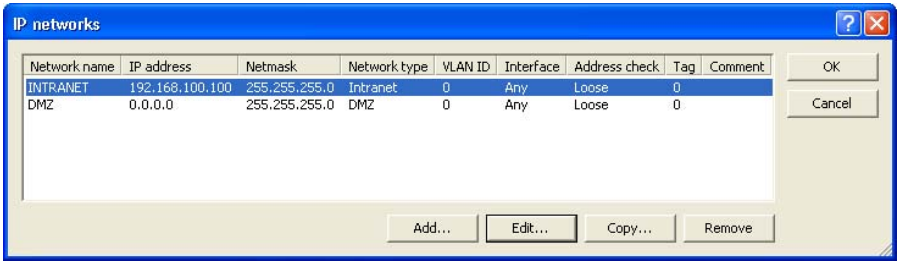


☐ Change the Device name to 'RIGHT'.

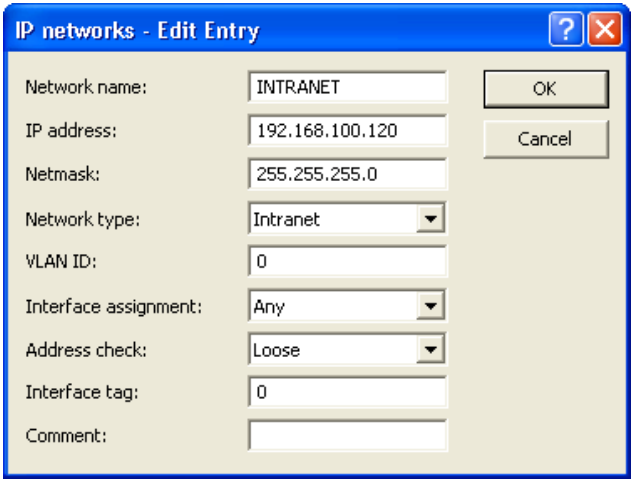
☐ Open the `Configuration : IPv4 : General` dialog.


Own addresses
In this table you can define IP networks. Those will be referenced by other modules (DHCP server, RIP, NetBIOS etc.) via the network name.
IP networks
You can configure alternative addresses at this table.
Loopback addresses
Options

☐ Click the 'IP networks...' button (above) to open the 'IP networks' window (below):



☐ In the ‘IP networks’ window (above), select the INTRANET network, then click the ’Edit...’ button to open the ‘Edit Entry’ dialog (below):



☐ In the ‘Edit Entry’ dialog, change the IP address of the RIGHT device configuration file to ’192.168.100.120’.

☐ Click ’OK’ twice in order to close the two open dialogs. Leave the configuration file open for later editing.

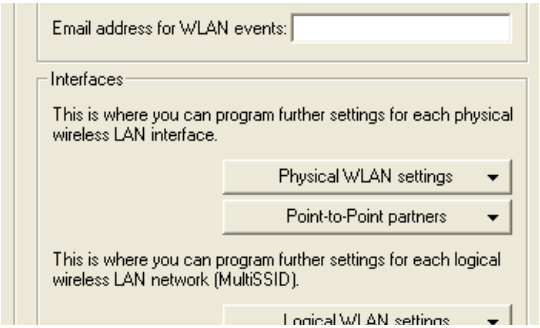
3.7.2 Configure the LEFT Device

The next task is to configure the LEFT device by:

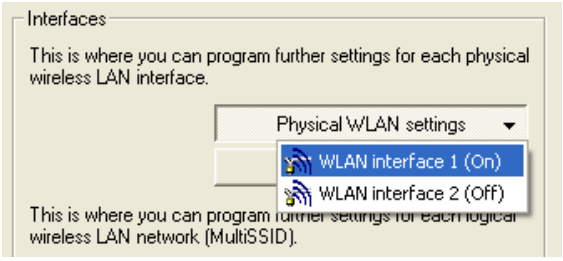
– enabling a single interface
– enabling a single channel on that interface

– designating the LEFT device as a slave
– identifying the MIDDLE device as its Point-to-Point partner

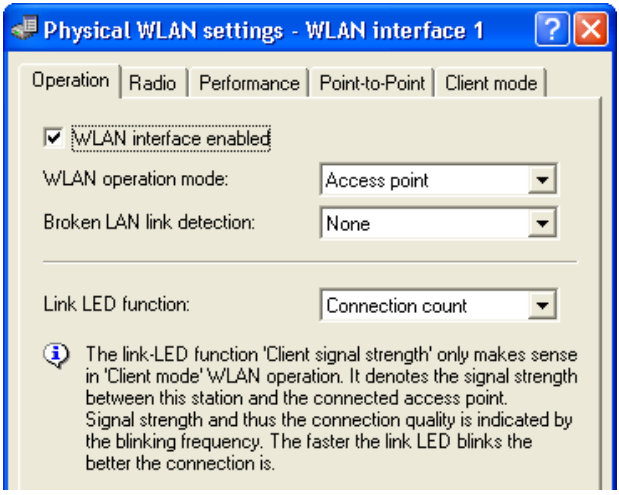
☐ In the `P2P-Relay-1Radio-LEFT.lcf` file, open the `Configuration : Wireless LAN : General` dialog (below):


Email address for WLAN events:
Interfaces
This is where you can program further settings for each physical wireless LAN interface.
Physical WLAN settings
Point-to-Point partners
This is where you can program further settings for each logical wireless LAN network (MultiSSID).

☐ Click the 'Physical WLAN settings' button, and select 'WLAN interface 1', as depicted below:

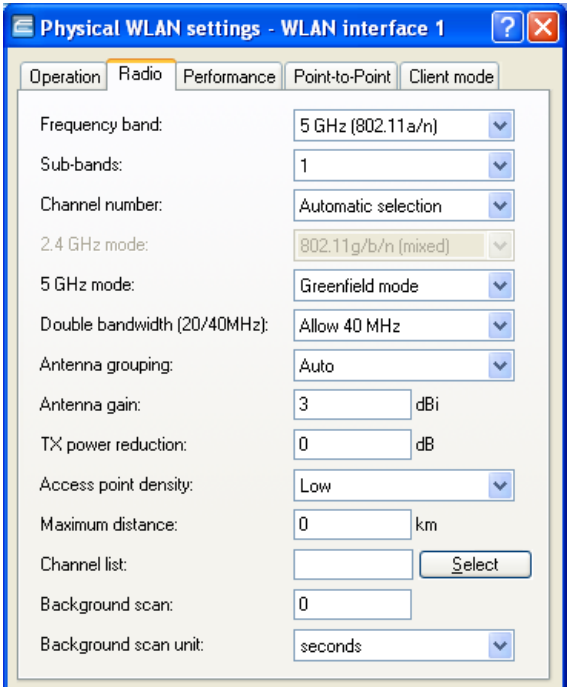

Interfaces
This is where you can program further settings for each physical wireless LAN interface.
Physical WLAN settings
WLAN interface 1 (On)
WLAN interface 2 (Off)
wireless LAN network (MultiSSID).

☐ In the WLAN Interface 1 window, click on the 'Operation' tab (below):


Physical WLAN settings - WLAN interface 1
Operation
Radio
Performance
Point-to-Point
Client mode
WLAN interface enabled
WLAN operation mode:
Access point
Broken LAN link detection:
None
Link LED function:
Connection count
The link-LED function 'Client signal strength' only makes sense in 'Client mode' WLAN operation. It denotes the signal strength between this station and the connected access point. Signal strength and thus the connection quality is indicated by the blinking frequency. The faster the link LED blinks the better the connection is.

Confirm that ’WLAN interface enabled’ is selected.

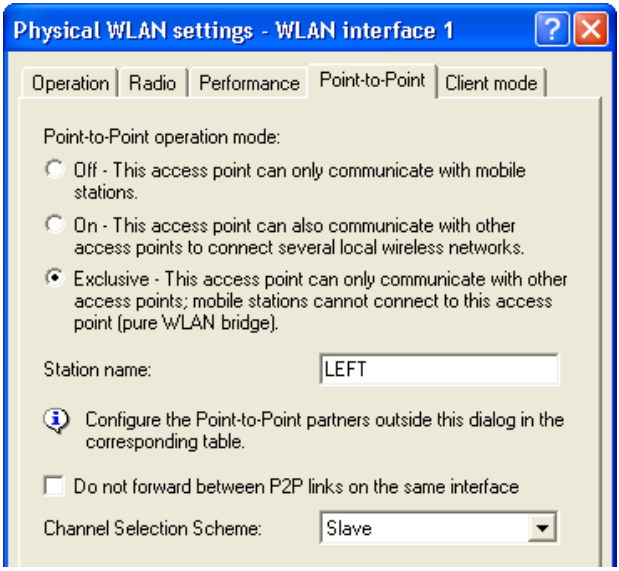
☐ Open the ’Radio’ tab (below) of the same dialog:



Edit the following properties:

– Frequency band: 5 GHz (802.11a/n)
– 5 GHz mode: Greenfield mode
– Antenna gain 9 dBi

☐ Click on the ’Point-to-Point’ tab (above) to open that dialog:

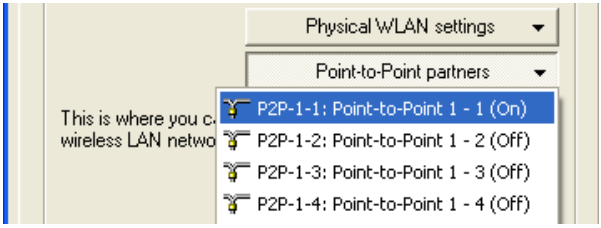

Physical WLAN settings - WLAN interface 1
Operation
Radio
Performance
Point-to-Point
Client mode
Point-to-Point operation mode:
Off - This access point can only communicate with mobile stations.
On - This access point can also communicate with other access points to connect several local wireless networks.
Exclusive - This access point can only communicate with other access points; mobile stations cannot connect to this access point (pure WLAN bridge).
Station name:
LEFT
Configure the Point-to-Point partners outside this dialog in the corresponding table.
Do not forward between P2P links on the same interface
Channel Selection Scheme:
Slave

In the Point-to-Point tab, enter the following settings:

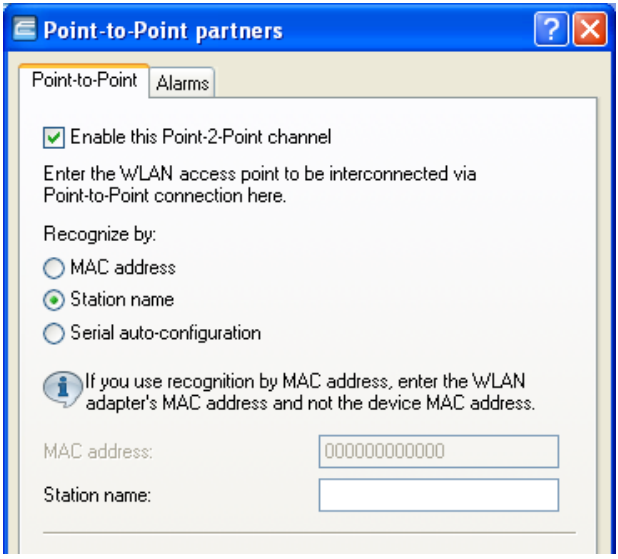
- Point-to-Point operation mode: 'Exclusive'
- Station name: 'LEFT'
- Channel Selection Scheme: 'Slave'

Click 'OK' to close the dialog.

☐ In the `Configuration: Wireless LAN : General` dialog, click the 'Point-to-Point partners' button, then select 'P2P-1-1' as depicted below:


Physical WLAN settings
Point-to-Point partners
This is where you c
wireless LAN netwo
P2P-1-1: Point-to-Point 1 - 1 (On)
P2P-1-2: Point-to-Point 1 - 2 (Off)
P2P-1-3: Point-to-Point 1 - 3 (Off)
P2P-1-4: Point-to-Point 1 - 4 (Off)

☐ The ‘Point-to-Point partners’ dialog opens, displaying settings for P2P interface 1, channel 1 (below):


Point-to-Point partners
Point-to-Point
Alarms
Enable this Point-2-Point channel
Enter the WLAN access point to be interconnected via Point-to-Point connection here.
Recognize by:
MAC address
Station name
Serial auto-configuration
If you use recognition by MAC address, enter the WLAN adapter's MAC address and not the device MAC address.
MAC address:
000000000000
Station name:

Enter the following settings:

– Select ’Enable this Point-2-Point channel’
– Select the ’Recognize by Station name’ option
– Change the Station name to: ’MIDDLE’

Click ’OK’ to close the ‘Point-to-Point partners’ dialog.

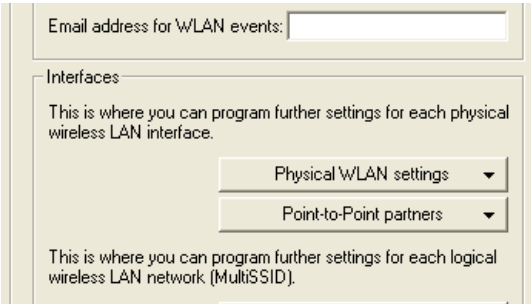
Click ’OK’ again to save configuration settings for the LEFT device.

3.7.3 Configure the MIDDLE Device

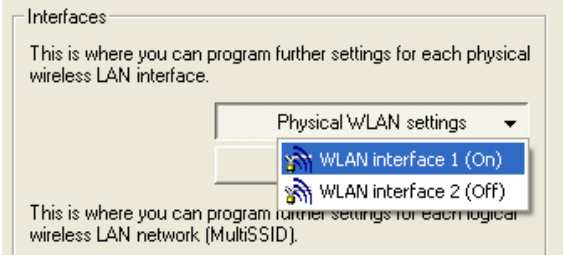
The next task is to configure the MIDDLE device by:

- enabling a single interface
- enabling two channels on that interface
- designating the MIDDLE device as the MASTER for each channel
- identifying the LEFT device as the Point-to-Point partner on channel 1
- identifying the RIGHT device as the Point-to-Point partner on channel 2

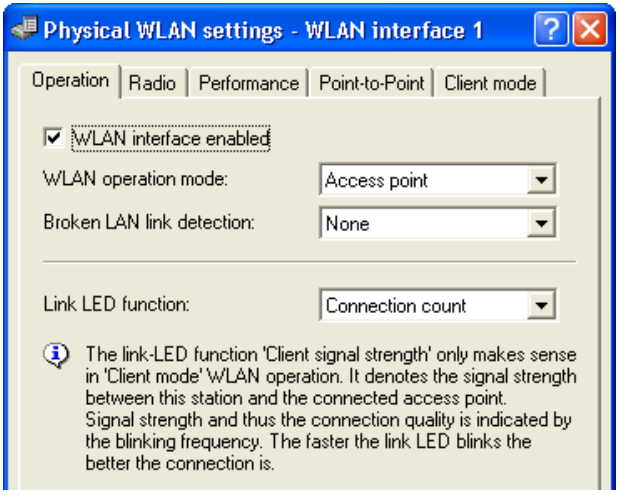
☐ In the `P2P-Relay-1Radio-MIDDLE.lcf` file, open the `Configuration : Wireless LAN : General` dialog (below):


Email address for WLAN events:
Interfaces
This is where you can program further settings for each physical wireless LAN interface.
Physical WLAN settings
Point-to-Point partners
This is where you can program further settings for each logical wireless LAN network (MultiSSID).

☐ Click on the 'Physical WLAN settings' button, and select 'WLAN interface 1', as depicted below:

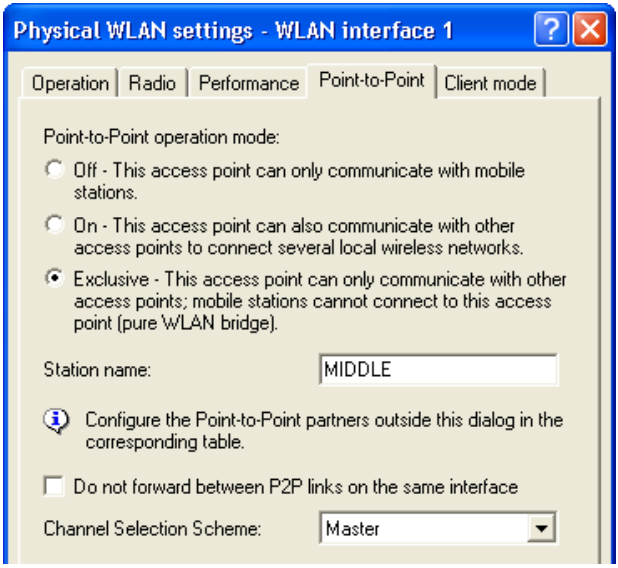

Interfaces
This is where you can program further settings for each physical wireless LAN interface.
Physical WLAN settings
WLAN interface 1 (On)
WLAN interface 2 (Off)
wireless LAN network (MultiSSID).

☐ In the 'WLAN Interface 1' dialog, click on the 'Operation' tab (below):


Physical WLAN settings - WLAN interface 1
Operation
Radio
Performance
Point-to-Point
Client mode
WLAN interface enabled
WLAN operation mode:
Access point
Broken LAN link detection:
None
Link LED function:
Connection count
The link-LED function 'Client signal strength' only makes sense in 'Client mode' WLAN operation. It denotes the signal strength between this station and the connected access point. Signal strength and thus the connection quality is indicated by the blinking frequency. The faster the link LED blinks the better the connection is.

Confirm that ’WLAN interface enabled’ is selected, then click the ’Point-to-Point’ tab.

☐ The ‘Point-to-Point’ dialog opens:

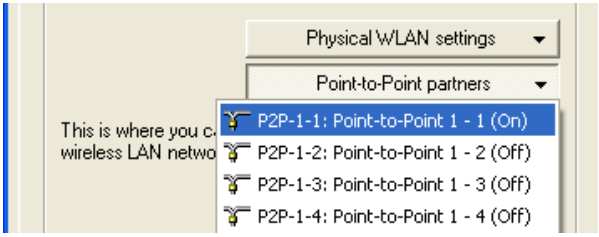

Physical WLAN settings - WLAN interface 1
Operation
Radio
Performance
Point-to-Point
Client mode
Point-to-Point operation mode:
Off - This access point can only communicate with mobile stations.
On - This access point can also communicate with other access points to connect several local wireless networks.
Exclusive - This access point can only communicate with other access points; mobile stations cannot connect to this access point (pure WLAN bridge).
Station name:
MIDDLE
Configure the Point-to-Point partners outside this dialog in the corresponding table.
Do not forward between P2P links on the same interface
Channel Selection Scheme:
Master

In the Point-to-Point tab, enter the following settings:

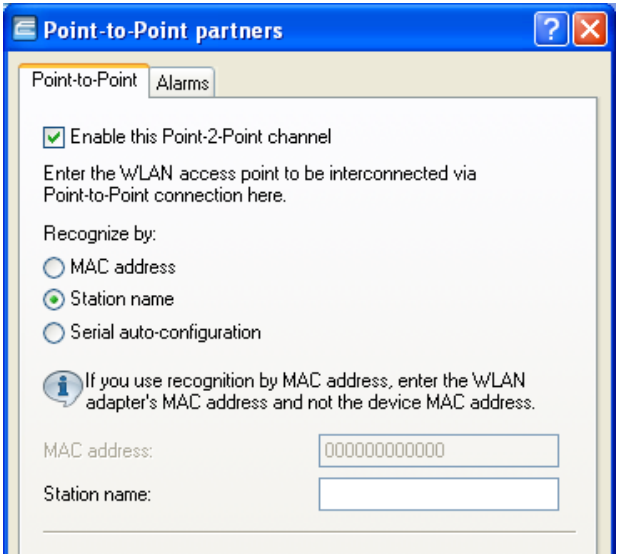
– Point-to-Point operation mode: 'Exclusive'
– Station name: 'MIDDLE'
– Channel Selection Scheme: 'Master'

Click 'OK'. The `Configuration : Wireless LAN : General` dialog opens. The next task is to identify the two point-to-point partners.

☐ Click the 'Point-to-Point partners' button, then select 'P2P-1-1' (interface 1, channel 1) as depicted below:


Physical WLAN settings
Point-to-Point partners
This is where you c
wireless LAN netwo
P2P-1-1: Point-to-Point 1 - 1 (On)
P2P-1-2: Point-to-Point 1 - 2 (Off)
P2P-1-3: Point-to-Point 1 - 3 (Off)
P2P-1-4: Point-to-Point 1 - 4 (Off)

☐ The 'Point-to-Point partners' dialog opens, displaying settings for P2P interface 1, channel 1 (below):

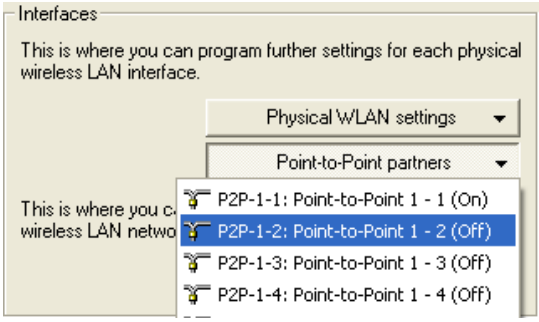

Point-to-Point partners
Point-to-Point
Alarms
Enable this Point-2-Point channel
Enter the WLAN access point to be interconnected via Point-to-Point connection here.
Recognize by:
MAC address
Station name
Serial auto-configuration
If you use recognition by MAC address, enter the WLAN adapter's MAC address and not the device MAC address.
MAC address:
000000000000
Station name:

In this dialog identify the LEFT device as the channel 1 Point-to-Point partner device:

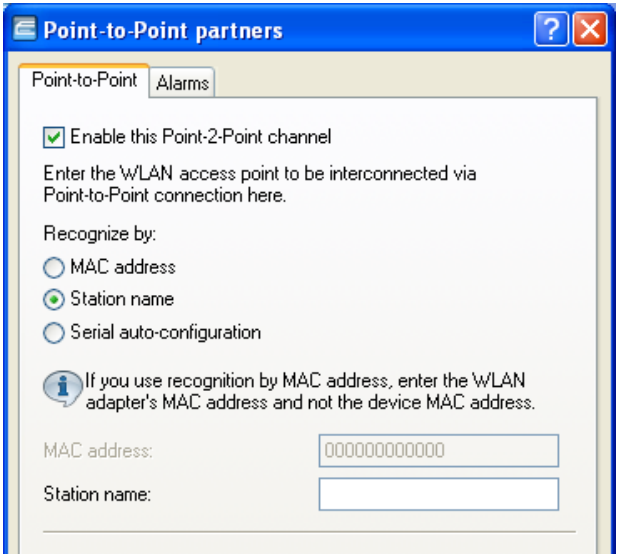
– Confirm that 'Enable this Point-2-Point channel' is selected
– Select 'Recognize by Station name'
– Change the partner Station name to 'LEFT'

Click 'OK' to close the 'Point-to-Point partners' dialog.

☐ In the `Configuration : Wireless LAN : General` dialog, click the 'Point-to-Point partners' button, then select 'P2P-1-2' (interface 1, channel 2) as depicted below:


Interfaces
This is where you can program further settings for each physical wireless LAN interface.
Physical WLAN settings
Point-to-Point partners
This is where you c
wireless LAN netwo
P2P-1-1: Point-to-Point 1 - 1 (On)
P2P-1-2: Point-to-Point 1 - 2 (Off)
P2P-1-3: Point-to-Point 1 - 3 (Off)
P2P-1-4: Point-to-Point 1 - 4 (Off)

☐ The ‘Point-to-Point partners’ dialog opens, displaying settings for P2P interface 1, channel 2 (below):


Point-to-Point partners
Point-to-Point
Alarms
Enable this Point-2-Point channel
Enter the WLAN access point to be interconnected via Point-to-Point connection here.
Recognize by:
MAC address
Station name
Serial auto-configuration
If you use recognition by MAC address, enter the WLAN adapter's MAC address and not the device MAC address.
MAC address:
000000000000
Station name:

In this dialog, identify the RIGHT device as the channel 2 Point-to-Point partner device:

– Select 'Enable this Point-2-Point channel'
– Select 'Recognize by Station name'
– Change the partner Station name to 'RIGHT'

Click 'OK' to close the 'Point-to-Point partners' dialog.

Click 'OK' a second time to save settings for the MIDDLE device.

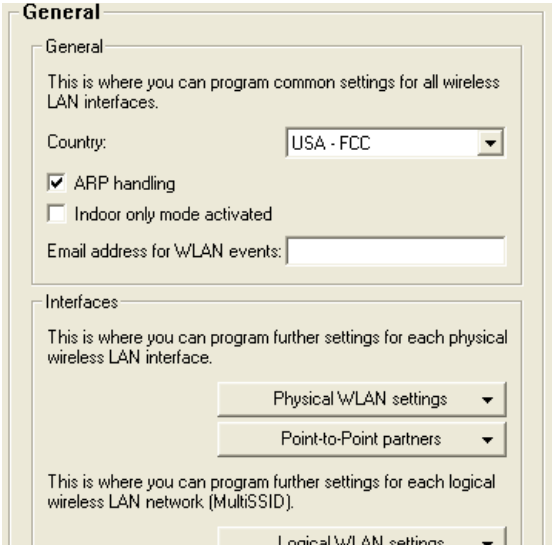
3.7.4 Configure the RIGHT Device

The next task is to configure the RIGHT device by:

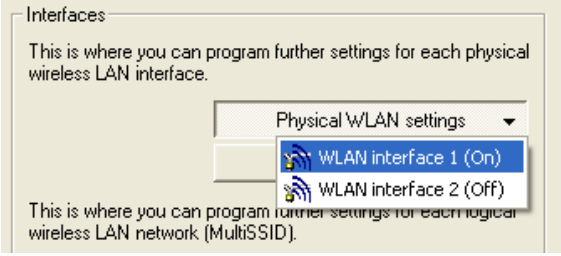
- enabling a single interface
- enabling a single channel on that interface

- designating the RIGHT device as a slave
- identifying the MIDDLE device as its Point-to-Point partner

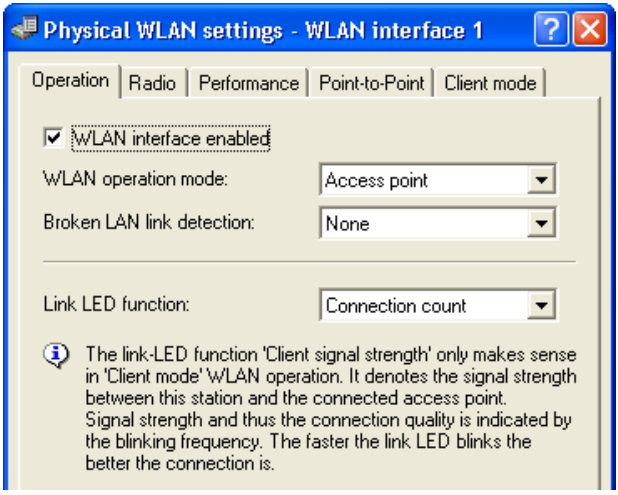
☐ In the `P2P-Relay-1Radio-RIGHT.lcf` file, open the `Configuration : Wireless LAN : General` dialog (below):


General
General
This is where you can program common settings for all wireless LAN interfaces.
Country:
USA - FCC
ARP handling
Indoor only mode activated
Email address for WLAN events:
Interfaces
This is where you can program further settings for each physical wireless LAN interface.
Physical WLAN settings
Point-to-Point partners
This is where you can program further settings for each logical wireless LAN network (MultiSSID).

☐ Click on the 'Physical WLAN settings' button, and select 'WLAN interface 1', as depicted below:

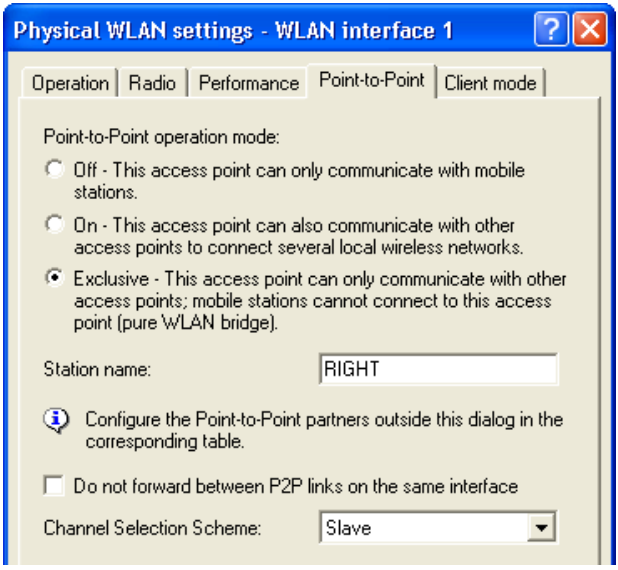

Interfaces
This is where you can program further settings for each physical wireless LAN interface.
Physical WLAN settings
WLAN interface 1 (On)
WLAN interface 2 (Off)
This is where you can program
wireless LAN network (MultiSSID).

☐ In the 'WLAN Interface 1' dialog, click on the 'Operation' tab (below):


Physical WLAN settings - WLAN interface 1
Operation
Radio
Performance
Point-to-Point
Client mode
WLAN interface enabled
WLAN operation mode:
Access point
Broken LAN link detection:
None
Link LED function:
Connection count
The link-LED function 'Client signal strength' only makes sense in 'Client mode' WLAN operation. It denotes the signal strength between this station and the connected access point. Signal strength and thus the connection quality is indicated by the blinking frequency. The faster the link LED blinks the better the connection is.

Confirm that 'WLAN interface enabled' is selected, then click on the 'Point-to-Point' tab.

☐ The 'Point-to-Point' dialog opens:

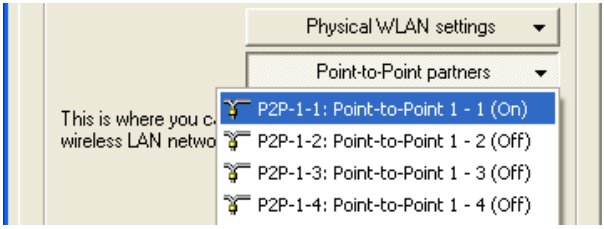

Physical WLAN settings - WLAN interface 1
Operation
Radio
Performance
Point-to-Point
Client mode
Point-to-Point operation mode:
Off - This access point can only communicate with mobile stations.
On - This access point can also communicate with other access points to connect several local wireless networks.
Exclusive - This access point can only communicate with other access points; mobile stations cannot connect to this access point (pure WLAN bridge).
Station name:
RIGHT
Configure the Point-to-Point partners outside this dialog in the corresponding table.
Do not forward between P2P links on the same interface
Channel Selection Scheme:
Slave

In the ‘Point-to-Point’ dialog, enter the following settings:

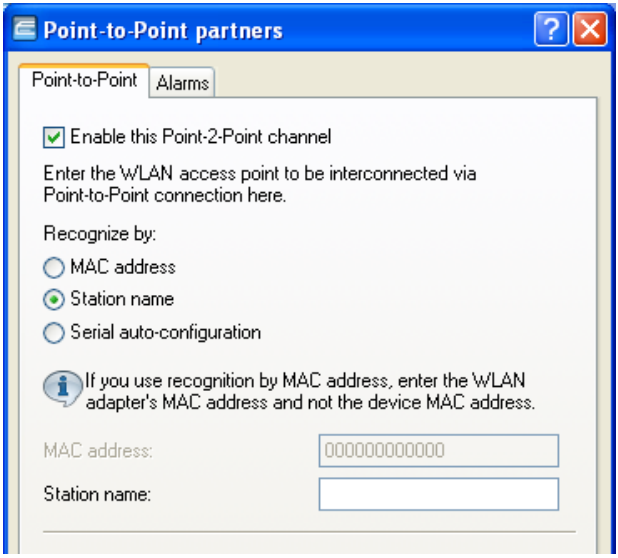
– Point-to-Point operation mode: ’Exclusive’
– Station name: ’RIGHT’
– Channel Selection Scheme: ’Slave’

Click ’OK’

☐ In the `Configuration : Wireless LAN : General` dialog, click the ’Point-to-Point partners’ button, then select ’P2P-1-1’ (interface 1, channel 1) as depicted below:


Physical WLAN settings
Point-to-Point partners
This is where you c
wireless LAN netwo
P2P-1-1: Point-to-Point 1 - 1 (On)
P2P-1-2: Point-to-Point 1 - 2 (Off)
P2P-1-3: Point-to-Point 1 - 3 (Off)
P2P-1-4: Point-to-Point 1 - 4 (Off)

☐ The ‘Point-to-Point partners’ dialog opens, displaying settings for P2P interface 1, channel 1 (below):


Point-to-Point partners
Point-to-Point
Alarms
Enable this Point-2-Point channel
Enter the WLAN access point to be interconnected via Point-to-Point connection here.
Recognize by:
MAC address
Station name
Serial auto-configuration
If you use recognition by MAC address, enter the WLAN adapter's MAC address and not the device MAC address.
MAC address:
000000000000
Station name:

Enter the following settings:

– Select ’Enable this Point-2-Point channel’
– Select ’Recognize by Station name’
– Station name: ’MIDDLE’

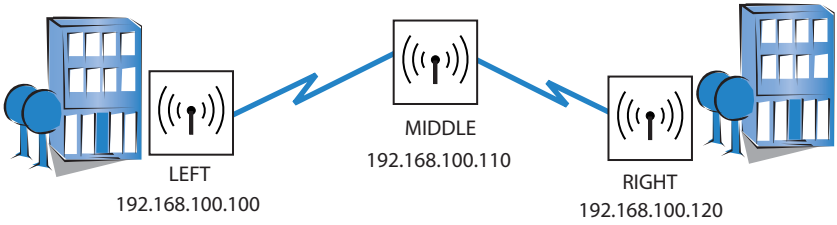
Click ’OK’ to close the ‘Point-to-Point partners’ dialog.

Click ’OK’ a second time to save settings for the CENTER device.

3.8 WLAN Bridge Relay: 2 Radios

This example employs three OpenBAT devices (named LEFT, CENTER, and RIGHT) to implement a WLAN bridge relay. All devices are located in the same subnet.

The CENTER device is a dual-radio device that serves as a repeater and relays messages between the LEFT and RIGHT devices. The CENTER device communicates with the LEFT device via radio interface 1, and with the RIGHT device via radio interface 2. Because the relay device uses just one channel per interface, 100% of the interface bandwidth for each connection.



The significant configuration settings for the device are as follows:

Station Name:	LEFT	CENTER	RIGHT
Role:	Access Point	Access Point	Access Point
IP address:	192,168,100,100	192,168,100,110	192,168,100,120
Subnet Mask:	255.255.255.0	255.255.255.0	255.255.255.0
Number of interfaces used:	1	2	1
Number of channels used:	1	2 (1 per interface)	1
Channel Selection Scheme	Master	Slave	Master
Point-to-Point Partner	CENTER-1	LEFT/RIGHT	CENTER-2

Each Access Point is configured to deny access to devices other than its immediate bridge partner. This example builds on the previous configurations of the RIGHT and LEFT(see on page 161), CENTER (see on page 167) and RIGHT(see on page 172) devices.

3.8.1 Creating Three LANconfig Files

Creating a WLAN bridge relay involves the creation and configuration of three LANconfig files, one for the LEFT device, one for the CENTER device, and one for the RIGHT device. Because each of these files contains virtually the same basic settings as the point-to-point relay example (1 radio) (see on page 155) , the easiest way to begin is to copy each of the 3 LANconfig files. After the files have been created, you can edit their configuration settings.

To create three new LANconfig files, follow these steps:

☐ Create a new LANconfig file: `P2P-Relay-2Radios-LEFT.lcf`:

- In Windows Explorer, navigate to the folder where the previously created LANconfig files are saved.
- Copy the file `P2P-Relay-1Radio-LEFT.lcf`.
- Paste the copied file into the same Windows Explorer folder.
- Rename the new file `P2P-Relay-2Radios-LEFT.lcf`.

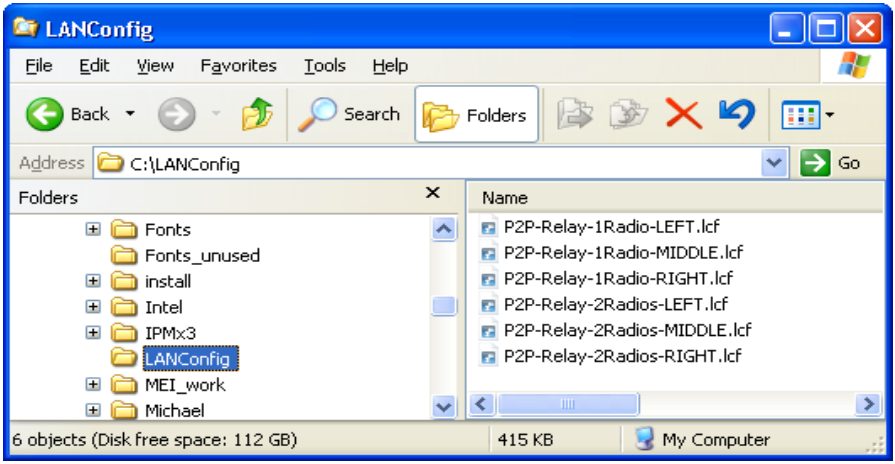
☐ Create a new LANconfig file: `P2P-Relay-2Radios-MIDDLE.lcf`:

- In Windows Explorer, navigate to the folder where the previously created LANconfig files are saved.
- Copy the file `P2P-Relay-1Radio-MIDDLE.lcf`.
- Paste the copied file into the same Windows Explorer folder.
- Rename the new file `P2P-Relay-2Radios-MIDDLE.lcf`.

☐ Create a new LANconfig file: `P2P-Relay-2Radios-RIGHT.lcf`.

- In Windows Explorer, navigate to the folder where the previously created LANconfig files are saved.
- Copy the file `P2P-Relay-1Radio-RIGHT.lcf`.
- Paste the copied file into the same Windows Explorer folder.
- Rename the new file `P2P-Relay-2Radios-RIGHT.lcf`.

Windows Explorer now contains the following files:



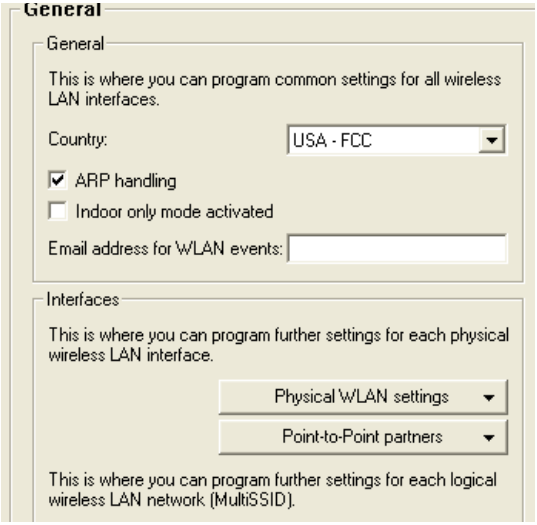
3.8.2 Configuring the MIDDLE Device

Most of the edits in this example are made to the MIDDLE device, which communicates to the LEFT and RIGHT devices via channels in separate radio interfaces. These edits include:

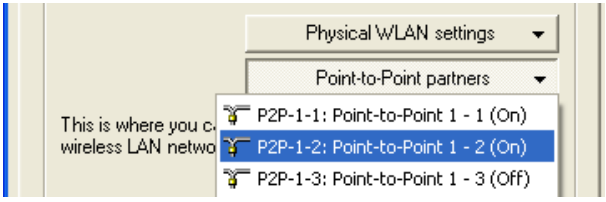
- Disabling Interface 1 / Channel 2
- Editing physical LAN settings for Interface 1
- Enabling and configuring Interface 2
- Enabling Interface 2 / Channel 1 and identifying a Point-to-Point partner
- Configuring encryption settings for Interface 2 / Channel 1

Disable Channel 2 on Interface 1

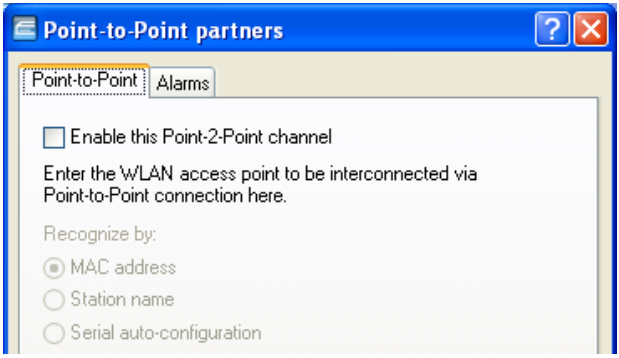
☐ In the `P2P-Relay-2Radios-MIDDLE.lcf` file, open the following dialog: `Configuration:Wireless LAN:General`.


General
General
This is where you can program common settings for all wireless LAN interfaces.
Country:
USA - FCC
ARP handling
Indoor only mode activated
Email address for WLAN events:
Interfaces
This is where you can program further settings for each physical wireless LAN interface.
Physical WLAN settings
Point-to-Point partners
This is where you can program further settings for each logical wireless LAN network (MultiSSID).

☐ Click on the 'Point-to-Point partners' button (above), then select 'P2P-1-2' (below):


Physical WLAN settings
Point-to-Point partners
P2P-1-1: Point-to-Point 1 - 1 (On)
P2P-1-2: Point-to-Point 1 - 2 (On)
P2P-1-3: Point-to-Point 1 - 3 (Off)

☐ The 'P2P-1-2 Point-to-Point partners' dialog opens:

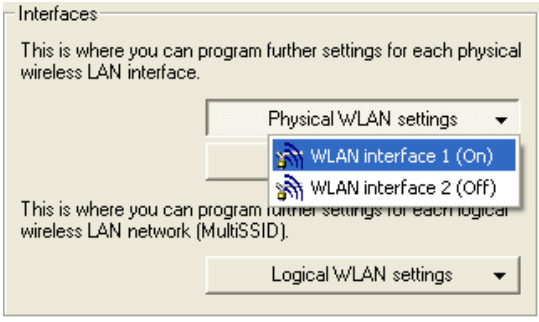


Disable Channel 2 of Interface 1 by de-selecting the checkbox (above).

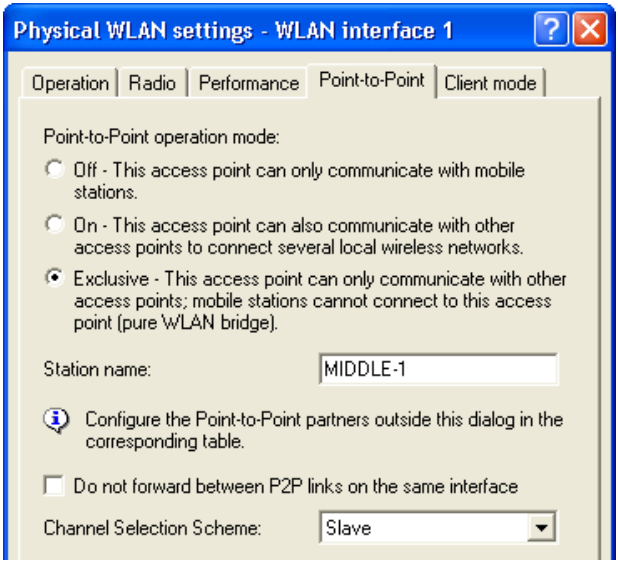
Click 'OK' to close this dialog.

Editing Physical LAN Settings for Interface 1

☐ In the `Configuration : Wireless LAN : General` dialog, click on the 'Physical WLAN settings' button, then select 'WLAN interface 1':


Interfaces
This is where you can program further settings for each physical wireless LAN interface.
Physical WLAN settings
WLAN interface 1 (On)
WLAN interface 2 (Off)
This is where you can program further settings for each logical wireless LAN network (MultiSSID).
Logical WLAN settings

☐ Open the 'Point-to-Point' tab of the WLAN Interface 1 dialog (below):


Physical WLAN settings - WLAN interface 1
Operation
Radio
Performance
Point-to-Point
Client mode
Point-to-Point operation mode:
Off - This access point can only communicate with mobile stations.
On - This access point can also communicate with other access points to connect several local wireless networks.
Exclusive - This access point can only communicate with other access points; mobile stations cannot connect to this access point (pure WLAN bridge).
Station name:
MIDDLE-1
Configure the Point-to-Point partners outside this dialog in the corresponding table.
Do not forward between P2P links on the same interface
Channel Selection Scheme:
Slave

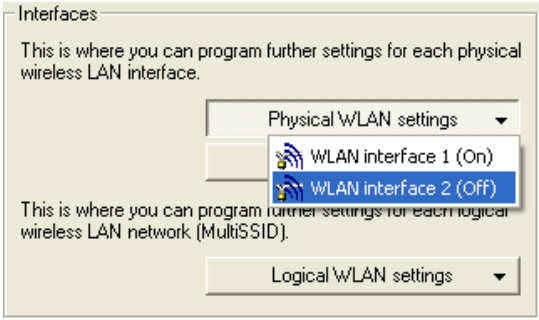
Make the following edits in the Point-to-Point dialog:

– Station name: ’MIDDLE-1’
– Channel Selection Scheme: ’Slave’

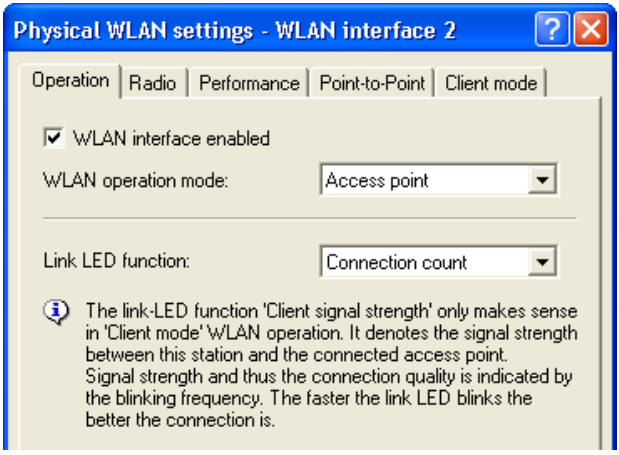
Click ’OK’.

Enabling and Configuring Interface 2

☐ Activate the PPPoE server in the `Configuration : Wireless-LAN : General` dialog, click on the 'Physical WLAN settings' button, then select 'WLAN interface 2', as shown below:

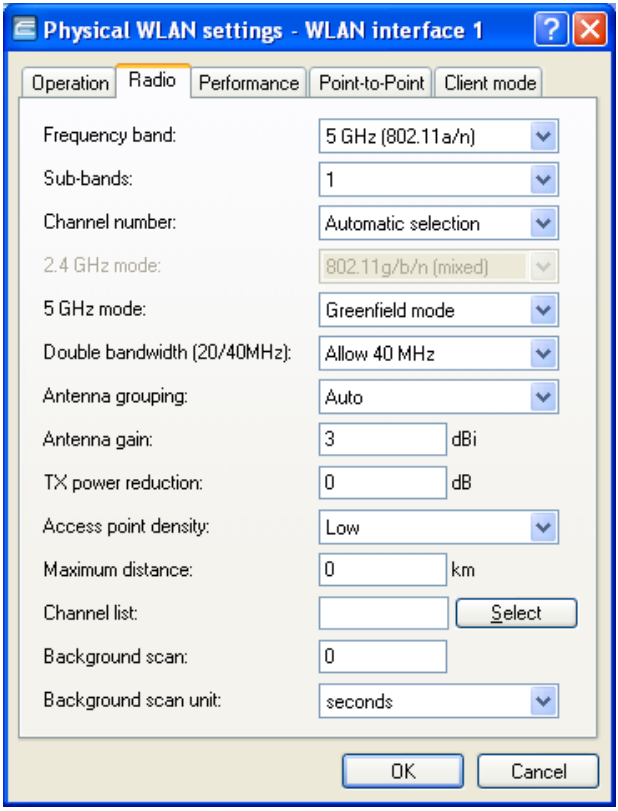

Interfaces
This is where you can program further settings for each physical wireless LAN interface.
Physical WLAN settings
WLAN interface 1 (On)
WLAN interface 2 (Off)
This is where you can program
wireless LAN network (MultiSSID).
Logical WLAN settings

☐ Open the 'Operation' tab (below) of the WLAN interface 2 dialog:


Physical WLAN settings - WLAN interface 2
Operation
Radio
Performance
Point-to-Point
Client mode
WLAN interface enabled
WLAN operation mode:
Access point
Link LED function:
Connection count
The link-LED function 'Client signal strength' only makes sense in 'Client mode' WLAN operation. It denotes the signal strength between this station and the connected access point.
Signal strength and thus the connection quality is indicated by the blinking frequency. The faster the link LED blinks the better the connection is.

Select 'WLAN interface enabled'.

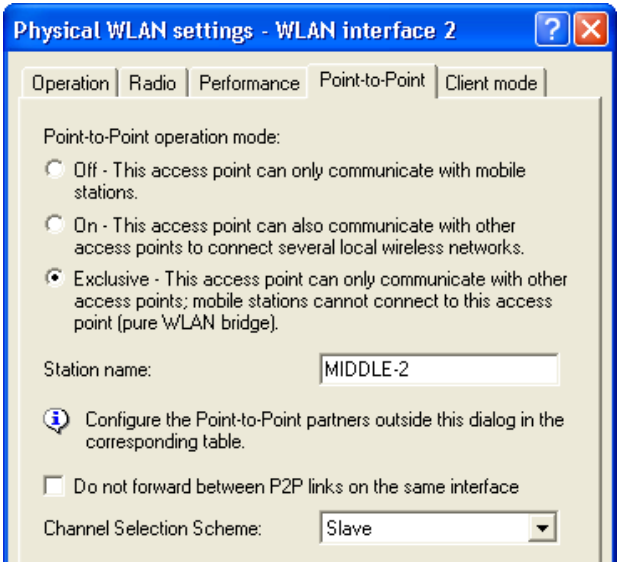
☐ Open the 'Radio' tab (below) of the same dialog:



Edit the following properties:

– Frequency band: 5 GHz (802.11a/n)
– 5 GHz mode: Greenfield mode
– Antenna gain 9 dBi

☐ Open the 'Point-to-Point' tab (below) in the same dialog:


Physical WLAN settings - WLAN interface 2
Operation
Radio
Performance
Point-to-Point
Client mode
Point-to-Point operation mode:
Off - This access point can only communicate with mobile stations.
On - This access point can also communicate with other access points to connect several local wireless networks.
Exclusive - This access point can only communicate with other access points; mobile stations cannot connect to this access point (pure WLAN bridge).
Station name:
MIDDLE-2
Configure the Point-to-Point partners outside this dialog in the corresponding table.
Do not forward between P2P links on the same interface
Channel Selection Scheme:
Slave

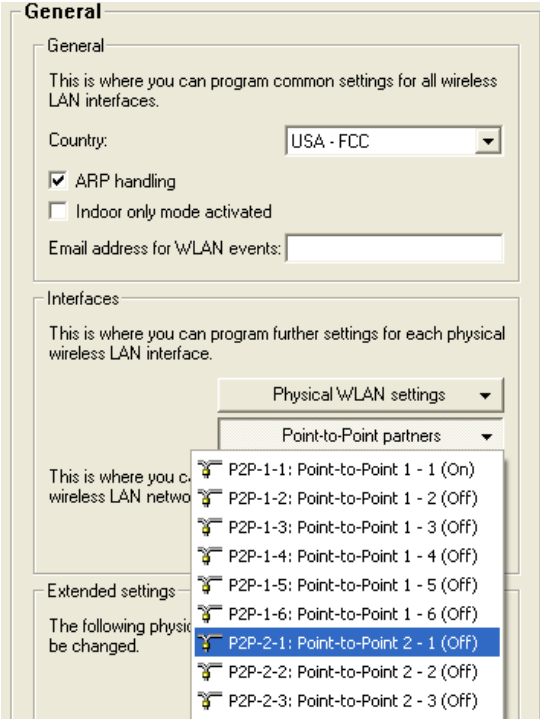
Make the following edits:

– Point-to-Point operation mode: ’Exclusive’
– Station name: ’MIDDLE-2’
– Channel Selection Scheme: ’Slave’

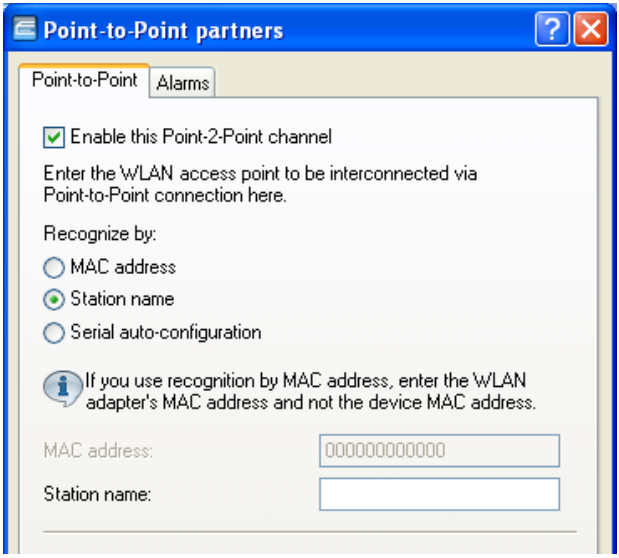
Click ’OK’.

Enabling Channel 1 on Interface 2; Specifying a P2P Partner

☐ In the `Configuration : Wireless LAN : General` dialog, click on the 'Point-to-Point partners' button, then select 'P2P-2-1, as depicted below:


General
General
This is where you can program common settings for all wireless LAN interfaces.
Country:
USA - FCC
ARP handling
Indoor only mode activated
Email address for WLAN events:
Interfaces
This is where you can program further settings for each physical wireless LAN interface.
Physical WLAN settings
Point-to-Point partners
P2P-1-1: Point-to-Point 1 - 1 (On)
P2P-1-2: Point-to-Point 1 - 2 (Off)
P2P-1-3: Point-to-Point 1 - 3 (Off)
P2P-1-4: Point-to-Point 1 - 4 (Off)
P2P-1-5: Point-to-Point 1 - 5 (Off)
P2P-1-6: Point-to-Point 1 - 6 (Off)
P2P-2-1: Point-to-Point 2 - 1 (Off)
P2P-2-2: Point-to-Point 2 - 2 (Off)
P2P-2-3: Point-to-Point 2 - 3 (Off)
Extended settings

☐ The P2P-2-1 Point-to-Point partners dialog (below) opens:


Point-to-Point partners
Point-to-Point
Alarms
Enable this Point-2-Point channel
Enter the WLAN access point to be interconnected via Point-to-Point connection here.
Recognize by:
MAC address
Station name
Serial auto-configuration
If you use recognition by MAC address, enter the WLAN adapter's MAC address and not the device MAC address.
MAC address:
000000000000
Station name:

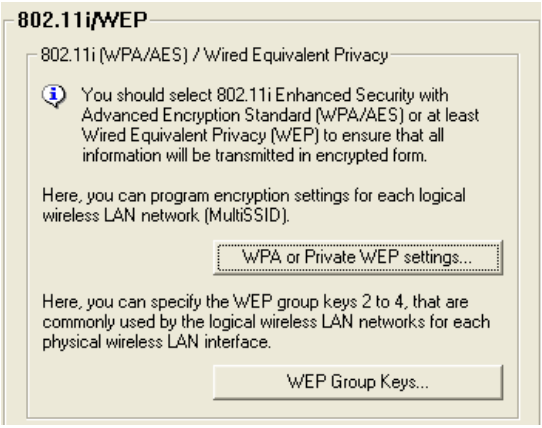
Use this dialog to enable this channel and identify the device that is the point-to-point partner of the MIDDLE device on this channel:

– Select ’Enable this Point-2-Point channel’, thereby enabling channel 1 of interface 2
– Recognize by: ’Station name’
– Station name: ’RIGHT’

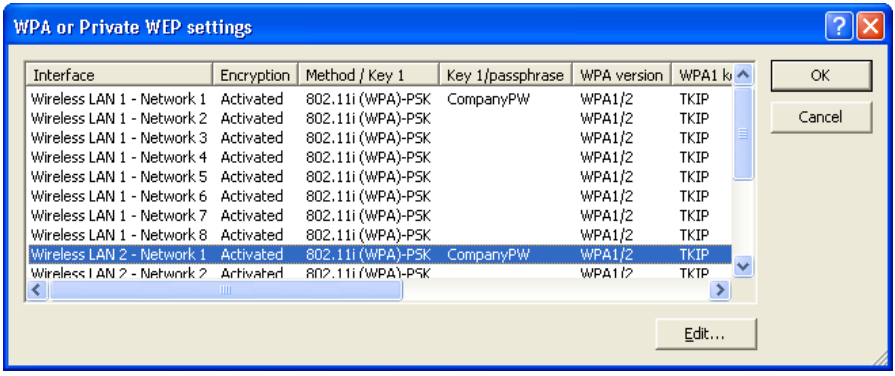
Click ’OK’.

Configure Encryption for Channel 1 on Interface 2

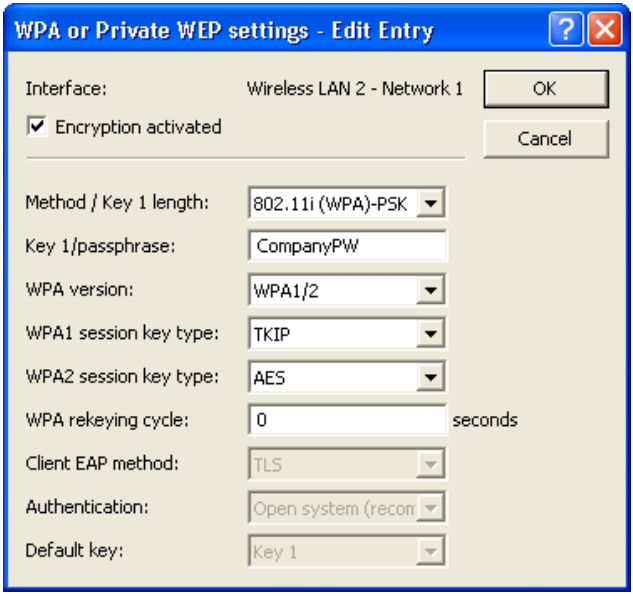
☐ Open the dialog
`Configuration : Wireless LAN : 802.11i/WEP`, below.


802.11i/WEP
802.11i (WPA/AES) / Wired Equivalent Privacy
You should select 802.11i Enhanced Security with Advanced Encryption Standard (WPA/AES) or at least Wired Equivalent Privacy (WEP) to ensure that all information will be transmitted in encrypted form.
Here, you can program encryption settings for each logical wireless LAN network (MultiSSID).
WPA or Private WEP settings...
Here, you can specify the WEP group keys 2 to 4, that are commonly used by the logical wireless LAN networks for each physical wireless LAN interface.
WEP Group Keys...

☐ Click on the 'WPA or Private WEP settings...' button (above) to open a list of networks (below):


WPA or Private WEP settings
Interface | Encryption | Method / Key 1 | Key 1/passphrase | WPA version | WPA1 k
Wireless LAN 1 - Network 1 | Activated | 802.11i (WPA)-PSK | CompanyPW | WPA1/2 | TKIP
Wireless LAN 1 - Network 2 | Activated | 802.11i (WPA)-PSK | | WPA1/2 | TKIP
Wireless LAN 1 - Network 3 | Activated | 802.11i (WPA)-PSK | | WPA1/2 | TKIP
Wireless LAN 1 - Network 4 | Activated | 802.11i (WPA)-PSK | | WPA1/2 | TKIP
Wireless LAN 1 - Network 5 | Activated | 802.11i (WPA)-PSK | | WPA1/2 | TKIP
Wireless LAN 1 - Network 6 | Activated | 802.11i (WPA)-PSK | | WPA1/2 | TKIP
Wireless LAN 1 - Network 7 | Activated | 802.11i (WPA)-PSK | | WPA1/2 | TKIP
Wireless LAN 1 - Network 8 | Activated | 802.11i (WPA)-PSK | | WPA1/2 | TKIP
Wireless LAN 2 - Network 1 | Activated | 802.11i (WPA)-PSK | CompanyPW | WPA1/2 | TKIP
OK
Cancel
Edit...

☐ In the network list, select 'Wireless LAN 2 - Network 1' (above), then click 'Edit...'. The 'Edit Entry' dialog opens (below):



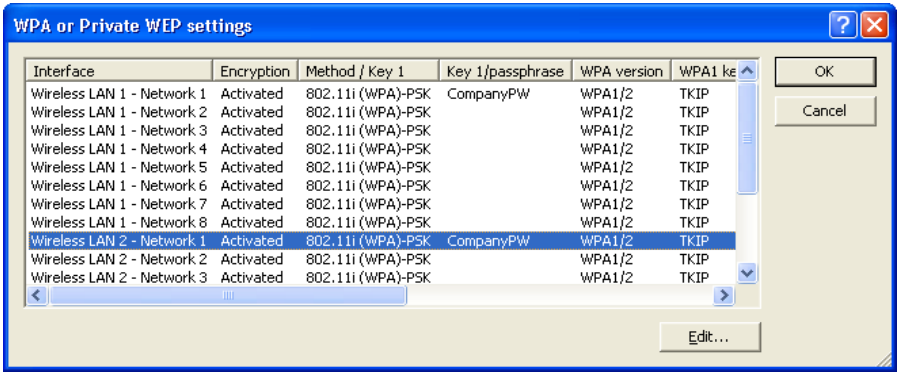
In the ‘Edit Entry’ dialog, enter the following settings for the encryption of the Interface 2 / Channel 1 network:

– Select ’Encryption activated’
– Method/Key 1 length: ’802.11i (WPA)-PSK’
– Key 1/passphrase: ’CompanyPW’

Accept the default settings for the remaining fields.

Click ’OK’ to close the dialog and return to the network list.

☐ The network list now displays P2P-2-1 as an activated network:


WPA or Private WEP settings
Interface
Encryption
Method / Key 1
Key 1/passphrase
WPA version
WPA1 ke
Wireless LAN 1 - Network 1 Activated 802.11i (WPA)-PSK CompanyPW WPA1/2 TKIP
Wireless LAN 1 - Network 2 Activated 802.11i (WPA)-PSK WPA1/2 TKIP
Wireless LAN 1 - Network 3 Activated 802.11i (WPA)-PSK WPA1/2 TKIP
Wireless LAN 1 - Network 4 Activated 802.11i (WPA)-PSK WPA1/2 TKIP
Wireless LAN 1 - Network 5 Activated 802.11i (WPA)-PSK WPA1/2 TKIP
Wireless LAN 1 - Network 6 Activated 802.11i (WPA)-PSK WPA1/2 TKIP
Wireless LAN 1 - Network 7 Activated 802.11i (WPA)-PSK WPA1/2 TKIP
Wireless LAN 1 - Network 8 Activated 802.11i (WPA)-PSK WPA1/2 TKIP
Wireless LAN 2 - Network 1 Activated 802.11i (WPA)-PSK CompanyPW WPA1/2 TKIP
Wireless LAN 2 - Network 2 Activated 802.11i (WPA)-PSK WPA1/2 TKIP
Wireless LAN 2 - Network 3 Activated 802.11i (WPA)-PSK WPA1/2 TKIP
OK
Cancel
Edit...

Click ’OK’ to close the window.

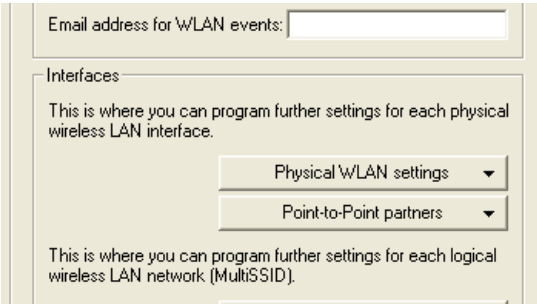
Click ’OK’ again to close the `P2P-Relay-2Radios-MIDDLE.lcf` file and save your configuration settings.

3.8.3 Configuring the LEFT Device

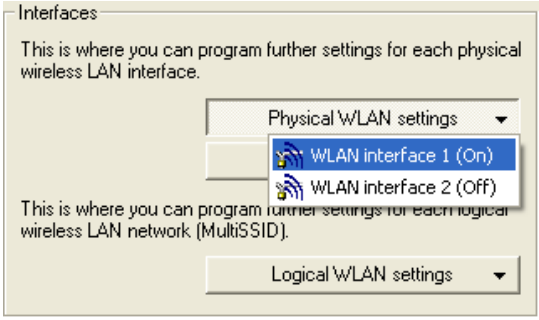
Configuring the LEFT device for service as part of a WLAN Bridge Relay is a much simpler task. The settings for this configuration are almost the same as for the LEFT device in a single radio relay design (see on page 161). Make the following configuration changes:

- Designate the LEFT device as the Master of the Point-to-Point link.
- Identify the MIDDLE-1 station as the LEFT device's Point-to-Point partner.

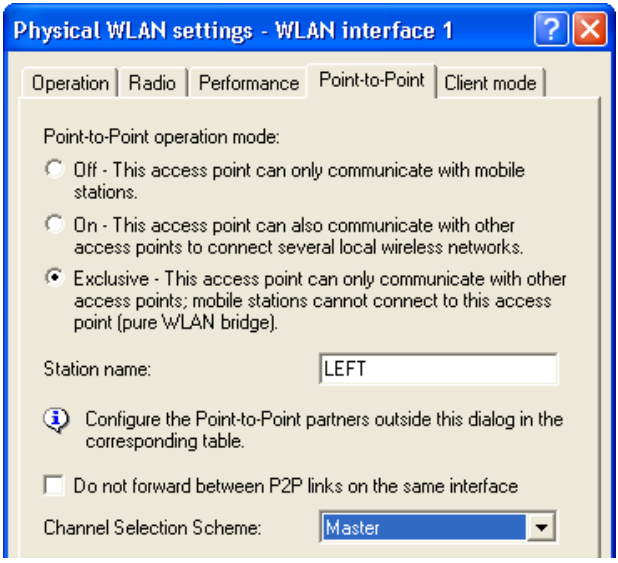
☐ Open the `P2P-Relay-2Radios-LEFT.lcf` file to the `Configuration : Wireless LAN : General` dialog:


Email address for WLAN events:
Interfaces
This is where you can program further settings for each physical wireless LAN interface.
Physical WLAN settings
Point-to-Point partners
This is where you can program further settings for each logical wireless LAN network (MultiSSID).

☐ Click on the 'Physical WLAN settings' button, then select 'WLAN interface 1' (below):


Interfaces
This is where you can program further settings for each physical wireless LAN interface.
Physical WLAN settings
WLAN interface 1 (On)
WLAN interface 2 (Off)
wireless LAN network (MultiSSID).
Logical WLAN settings

☐ Open the 'Point-to-Point' tab of this dialog (below):


Physical WLAN settings - WLAN interface 1
Operation
Radio
Performance
Point-to-Point
Client mode
Point-to-Point operation mode:
Off - This access point can only communicate with mobile stations.
On - This access point can also communicate with other access points to connect several local wireless networks.
Exclusive - This access point can only communicate with other access points; mobile stations cannot connect to this access point (pure WLAN bridge).
Station name:
LEFT
Configure the Point-to-Point partners outside this dialog in the corresponding table.
Do not forward between P2P links on the same interface
Channel Selection Scheme:
Master

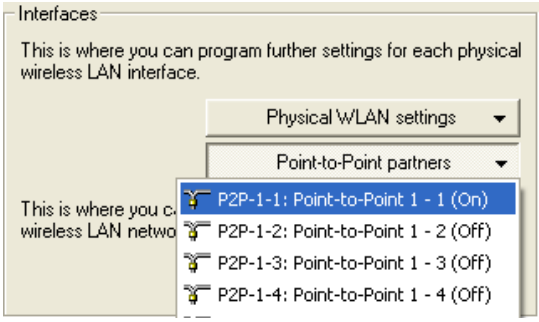
Make the following edits:

– Channel Selection Scheme: 'Master'

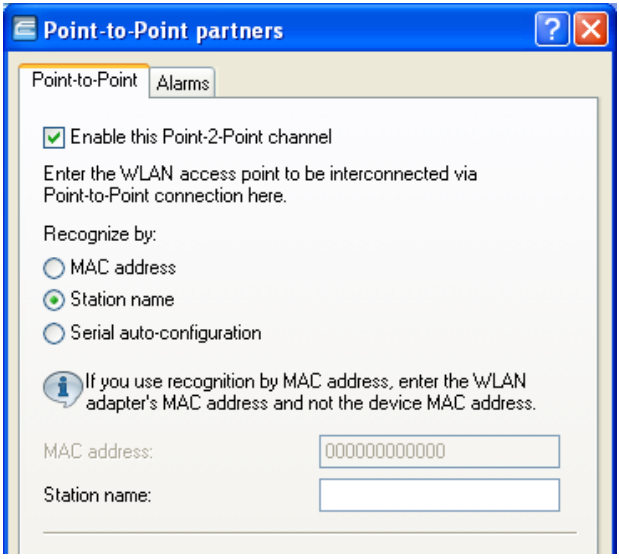
Leave the other settings in this dialog unchanged.

Click 'OK' to close the dialog.

☐ In the `Configuration : Wireless LAN : General` dialog, click the 'Point-to-Point partners' button, then select 'P2P-1-1' (below):


Interfaces
This is where you can program further settings for each physical wireless LAN interface.
Physical WLAN settings
Point-to-Point partners
This is where you c
wireless LAN netwo
P2P-1-1: Point-to-Point 1 - 1 (On)
P2P-1-2: Point-to-Point 1 - 2 (Off)
P2P-1-3: Point-to-Point 1 - 3 (Off)
P2P-1-4: Point-to-Point 1 - 4 (Off)

☐ In the Point-to-Point partners dialog, change the Station name to 'CENTER-1'.


Point-to-Point partners
Point-to-Point
Alarms
Enable this Point-2-Point channel
Enter the WLAN access point to be interconnected via Point-to-Point connection here.
Recognize by:
MAC address
Station name
Serial auto-configuration
If you use recognition by MAC address, enter the WLAN adapter's MAC address and not the device MAC address.
MAC address:
000000000000
Station name:

Click 'OK' to close the dialog.

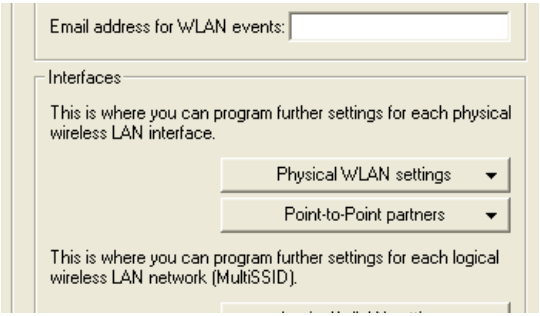
Click 'OK' again to close the `P2P-Relay-2Radios-LEFT.lcf` file and save your edits to the LEFT device.

3.8.4 Configuring the RIGHT Device

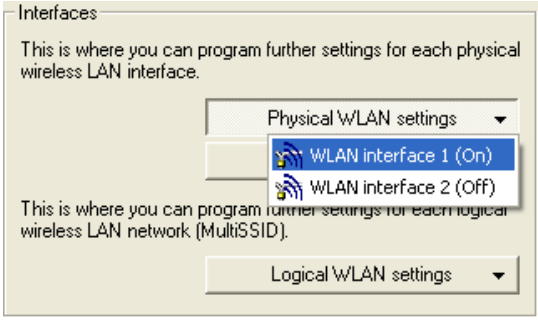
Configuring the RIGHT device for service as part of a WLAN Bridge Relay requires the virtually the same changes made to the LEFT device in the preceding section. Again, the settings for this configuration are almost the same as for the RIGHT device in a single radio relay design (see on page 172). Make the following configuration changes:

- Designate the RIGHT device as the Master of the Point-to-Point link.
- Identify the MIDDLE-2 station as the RIGHT device's Point-to-Point partner.

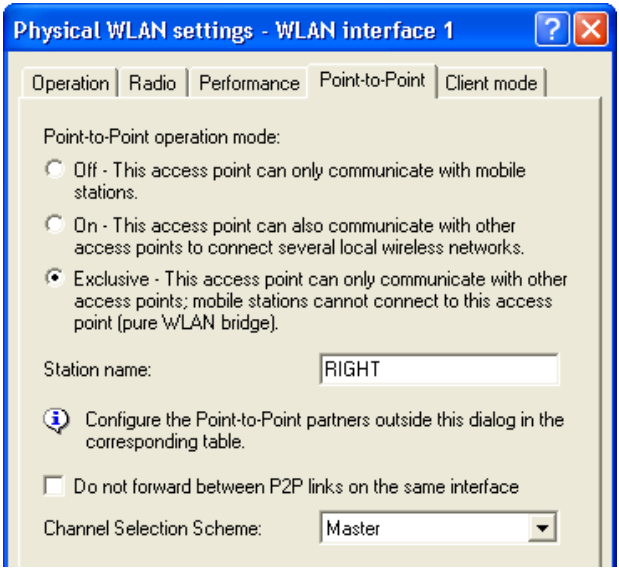
☐ In the `P2P-Relay-2Radios-RIGHT.lcf` file, open the following dialog: `Configuration:Wireless LAN:General`.


Email address for WLAN events:
Interfaces
This is where you can program further settings for each physical wireless LAN interface.
Physical WLAN settings
Point-to-Point partners
This is where you can program further settings for each logical wireless LAN network (MultiSSID).

☐ Click on the 'Physical WLAN settings' button, then select 'WLAN interface 1' (below):


Interfaces
This is where you can program further settings for each physical wireless LAN interface.
Physical WLAN settings
WLAN interface 1 (On)
WLAN interface 2 (Off)
wireless LAN network (MultiSSID).
Logical WLAN settings

☐ Open the 'Point-to-Point' tab of this dialog (below):


Physical WLAN settings - WLAN interface 1
Operation
Radio
Performance
Point-to-Point
Client mode
Point-to-Point operation mode:
Off - This access point can only communicate with mobile stations.
On - This access point can also communicate with other access points to connect several local wireless networks.
Exclusive - This access point can only communicate with other access points; mobile stations cannot connect to this access point (pure WLAN bridge).
Station name:
RIGHT
Configure the Point-to-Point partners outside this dialog in the corresponding table.
Do not forward between P2P links on the same interface
Channel Selection Scheme:
Master

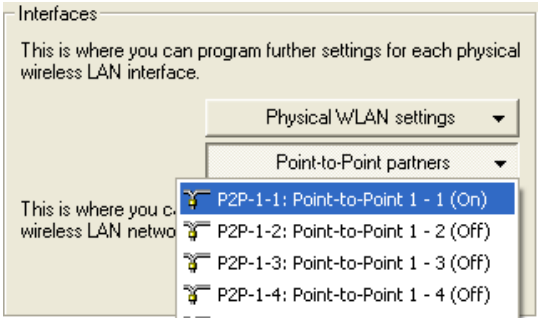
Make the following edits:

– Channel Selection Scheme: 'Master'

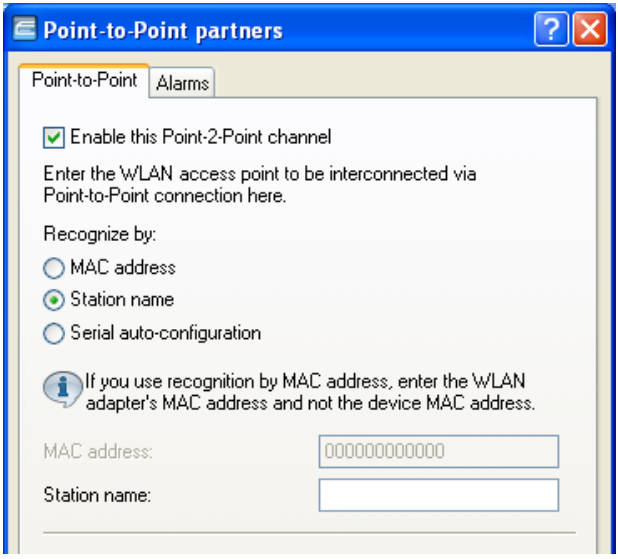
Leave the other settings in this dialog unchanged.

Click 'OK' to close this dialog.

☐ In the `Configuration : Wireless LAN : General` dialog, click the 'Point-to-Point partners' button, then select 'P2P-1-1' (below):


Interfaces
This is where you can program further settings for each physical wireless LAN interface.
Physical WLAN settings
Point-to-Point partners
This is where you c
wireless LAN netwo
P2P-1-1: Point-to-Point 1 - 1 (On)
P2P-1-2: Point-to-Point 1 - 2 (Off)
P2P-1-3: Point-to-Point 1 - 3 (Off)
P2P-1-4: Point-to-Point 1 - 4 (Off)

☐ In the Point-to-Point partners dialog, change the Station name to 'CENTER-2'.


Point-to-Point partners
Point-to-Point
Alarms
Enable this Point-2-Point channel
Enter the WLAN access point to be interconnected via Point-to-Point connection here.
Recognize by:
MAC address
Station name
Serial auto-configuration
If you use recognition by MAC address, enter the WLAN adapter's MAC address and not the device MAC address.
MAC address:
000000000000
Station name:

Click 'OK' to close this dialog.

Click 'OK' again to close the `P2P-Relay-2Radios-RIGHT.lcf` file and save your edits to the RIGHT device.

4 Central WLAN Management

In many areas, WLAN systems are suitable substitutes for or additions to wired networks. In some cases, WLANs even provide completely new application options that can enable major progress in organizing the work, or significant resource saving possibilities.

4.1 Application Examples

4.1.1 Managed Mode

The widespread use of wireless Access Points and wireless routers has resulted in a significantly more comfortable and flexible access to networks in companies, universities and other organizations. By employing central WLAN management in managed mode, Access Points are configured in a central instance, the WLAN-Controller.
The WLAN-Controller authenticates the Access Points and transfers a certificate and a matching configuration to the admitted devices. You can thus configure the wireless network comfortably from a central position and the configuration changes simultaneously affect all Access Points.
Using split management, you can separate the WLAN configuration from the remaining router configuration. This is how you can configure e.g. the router and VPN settings in branch offices or home offices. You can define the WLAN configuration via a Hirschmann WLAN Controller in the head office.

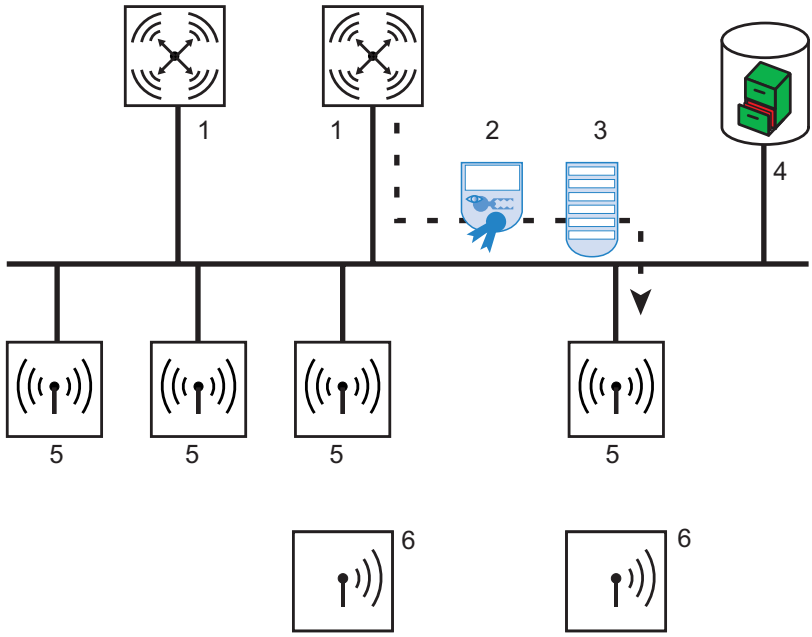


Figure 8: Configuring several Access Points with one WLAN Controller
1: WLAN Controller
2: Certificate
3: Configuration
4: Server
5: Access Point
6: WLAN Client

4.1.2 WLAN Bridge to Access Point – Managed and Unmanaged Mixed

The Access Points managed by a central WLAN Controller are usually directly connected to the wired Ethernet. If a direct connection is not possible, you can also integrate the managed Access Points via a WLAN bridge into the LAN, as far as they have 2 WLAN modules. In this application case, a WLAN module functions as managed Access Point. This WLAN module always retrieves its configuration centrally from the WLAN Controller. The other WLAN module functions as fixed WLAN bridge during this process.

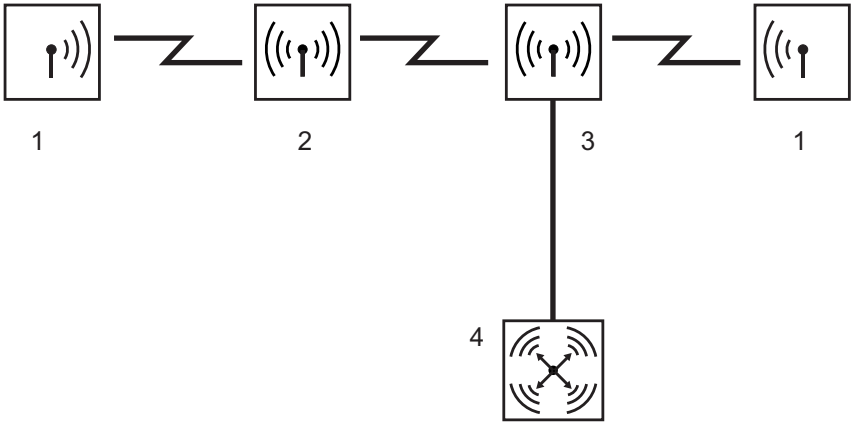


Figure 9: Mixed configuration with WLAN bridge to Access Point

4.2 Introduction

The widespread use of wireless Access Points and wireless routers has resulted in a significantly more comfortable and flexible access to networks in companies, universities and other organizations.
Despite all advantages of WLAN structures, there are still some open aspects to consider:

- ☐ All wireless Access Points must be configured and monitored correspondingly to detect unwanted WLAN Clients, etc. With larger WLAN structures and corresponding security mechanisms, high qualifications are needed for the administration of Access Points. Furthermore, persons in charge must be experienced and significant resources are tied down in IT departments.
- ☐ If the WLAN structure is changed, the manual adjustment of the Access-Point configuration might take a longer period of time. Therefore there will be different configurations in the WLAN at the same time.
- ☐ The joint use of the shared transfer medium (air) requires an effective coordination of the Access Points to avoid frequency overlaps and to optimize the network performance.
- ☐ Access Points in publicly accessible locations represent a potential security risk, as not only the devices, but also the security-relevant data stored in them, such as passwords, are exposed to the risk of theft. Also, third parties may connect external Access Points to the LAN unnoticed and thus bypass the valid security regulations.

A central WLAN management will resolve these problems. The Access Points are configured in a central instance, the WLAN Controller. The WLAN Controller authenticates the Access Points and transfers a matching configuration to the admitted devices. This permits you to configure the wireless network comfortably from a central position. The changes in configuration simultaneously affect all Access Points. The device saves the configuration assigned by the WLAN Controller in the Access Points optionally in the RAM instead of the flash memory. This will ensure that, with particularly security-critical networks, no security-relevant data will get into the hands of unauthorized persons if the devices are stolen. Exclusively in stand-alone operation will the device optionally save the configuration in the flash memory for a defined period of time. There is no possibility of accessing this memory area with LANconfig or other tools.

4.2.1 The CAPWAP Standard

With the Control And Provisioning of Wireless Access Points (CAPWAP protocol), the Internet Engineering Task Force (IETF) presents a draft standard for the central management of large WLAN structures.
CAPWAP uses 2 channels for data transfer:

- ☐ Control channel, DTLS-encrypted. This channel is used to exchange management information between WLAN Controller and Access Point.

  Note: Datagram Transport Layer Security (DTLS) is a TLS-based encryption protocol. It can also be used for transfers via connectionless, unsecured transport protocols, such as UDP. DTLS hence combines the advantages of the high security provided by TLS with the rapid transfer via UDP. Unlike TLS, DTLS is therefore also suitable for the transmission of VoIP packets, as the device can still authenticate the subsequent packets even after the loss of a packet.

- ☐ Data channel, optionally also DTLS-encrypted. The WLAN Controller transfers the WLAN payload data from the Access Point into the LAN - encapsulated in the CAPWAP protocol.

4.2.2 The Smart Controller Technology

A decentralized WLAN structure with autonomous Access Points (stand-alone operation referred to as "Rich Access Points") includes all functions for data transfer on the PHY layer, the control functions on the MAC layer and the management functions in the Access Points. The central WLAN management assigns these tasks to two different devices:

- ☐ The central WLAN Controller assumes the management tasks.
- ☐ The decentralized Access Points handle the data transfer on the PHP layer and the MAC functions.
- ☐ A RADIUS or EAP server may be added as a third component to authenticate the WLAN Clients. This is also possible in stand-alone wireless networks.

CAPWAP describes 3 different scenarios for the relocation of WLAN functions to the central WLAN Controller.

☐ Remote MAC: The device transfers all WLAN functions from the Access Point to the WLAN Controller. In this case, the Access Points serve exclusively as "extended antennas" without own intelligence.

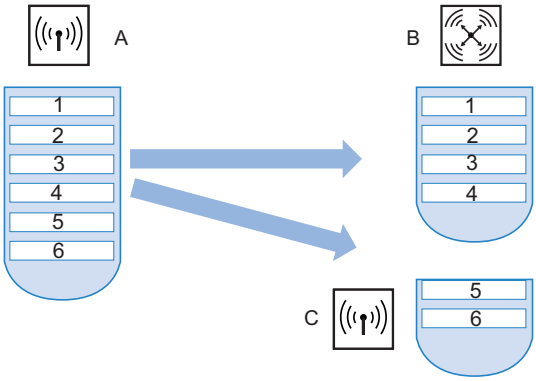


Figure 10: Split MAC in central WLAN management
A: Autonomous Access Point
B: WLAN Controller
C: Decentralized Access Point
1: Management
2: Authentication
3: Realtime MAC
4: Non-realtime MAC
5: PHY layer
6: Antenna

☐ Split MAC: With this variant, the WLAN Controller only obtains some of the WLAN functions. Usually the Access Point continues to perform the time-critical applications (realtime applications) and the applications that are not time-critical (non-realtime applications) will be performed by the central WLAN Controller.

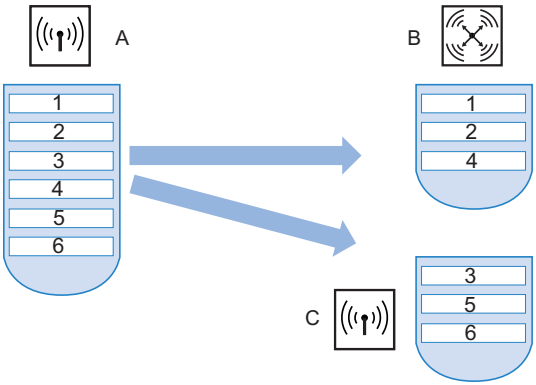


Figure 11: Split MAC in central WLAN management
A: Autonomous Access Point
B: WLAN Controller
C: Decentralized Access Point
1: Management
2: Authentication
3: Realtime MAC
4: Non-realtime MAC
5: PHY layer
6: Antenna

☐ Local MAC: The third option is the complete management and monitoring of the WLAN data traffic directly in the Access Points. The Access Point and the WLAN Controller merely exchange messages on ensuring a uniform configuration of the Access Points and on network management.

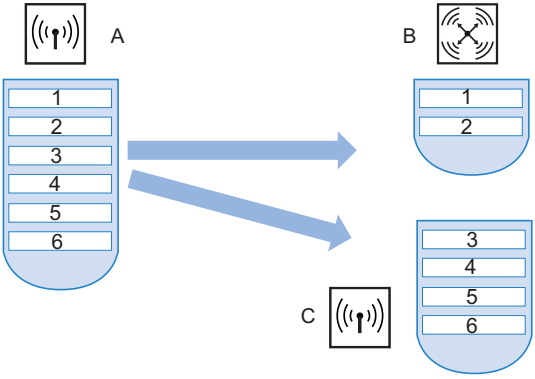


Figure 12: Local MAC with central WLAN management
A: Autonomous Access Point
B: WLAN Controller
C: Decentralized Access Point
1: Management
2: Authentication
3: Realtime MAC
4: Non-realtime MAC
5: PHY layer
6: Antenna

Hirschmann's smart controller technology employs the local MAC procedure. Through the reduction of centralized tasks, these WLAN structures offer optimum scalability. At the same time, such a structure prevents bottlenecks at the WLAN Controller, which processes large parts of the overall data traffic. Remote-MAC and split-MAC architectures always require centralized processing of all payload data in the WLAN Controller. In local-MAC architectures, the Access Points alternatively release the data directly into the LAN, permitting high-performance data transfer. This makes Hirschmann WLAN Controllers suitable for wireless networks complying with the IEEE 802.11n draft standard, offering significantly higher bandwidths than conventional wireless networks. Route the data directly into special VLANs when releasing them to the LAN. This makes it very easy to set up closed networks, e.g. for guest access accounts.

4.2.3 Communication between Access Point and WLAN-Controller

Communication between an Access Point and the WLAN-Controller is always initiated by the Access Point. In the following cases, the devices search for a WLAN-Controller that assigns them a configuration:

- ☐ A Hirschmann Access Point is still set to its factory default settings and has not been configured yet. In this state, the WLAN modules are switched off, the Access Point searches the LAN for a WLAN-Controller.
- ☐ A Hirschmann Access Point has already been configured, at least one WLAN module has been manually set to the operating mode 'managed'. The Access Point searches for a WLAN-Controller for the corresponding WLAN module(s) in the LAN.

At the beginning of the communication, the Access Point sends a "Discovery Request Message" to identify the available WLAN-Controllers. The device sends this request as broadcast. However, because in some structures, the Access Point cannot reach a potential WLAN-Controller via broadcast, define special addresses of additional WLAN-Controllers in the configuration of the Access Points.

Note: The device can also resolve DNS names of WLAN-Controllers. All Access Points with HiLCOS 7.22 or higher have the pre-configured default name 'WLC-Address' so that a DNS server can resolve this name to a Hirschmann WLAN Controller. The same applies to the DNS suffixes learned via DHCP. This also makes it possible to reach WLAN-Controllers that are located in the same network without having to configure the Access Points.

From the available WLAN-Controllers, the Access Point selects the best one and queries it for the structure of the DTLS connection. The "best" WLAN-Controller for the Access Point is the one with the least load, that is the one with the lowest rate of managed Access Points compared to the maximum possible Access Points. In case of 2 or more equally "good" WLAN-Controllers, the Access Point selects the nearest one in the network, i.e. the one with the shortest response time.

The WLAN-Controller then uses an internal random number to determine a unique and secure session key which it uses to protect the connection to the Access Point. The CA in the WLAN-Controller issues a certificate to the Access Point by means of SCEP. The certificate is protected as "challenge" by a password for one-time use only, the Access Point uses this certificate for authentication to the WLAN-Controller to collect the certificate.
The Access Point is provided with the configuration for the integrated SCEP client via the secure DTLS connection – the Access Point is then able to retrieve ts certificate from the SCEP CA via SCEP. Once this is done, the assigned configuration is transferred to the Access Point.

Note: SCEP stands for Simple Certificate Enrollment Protocol; CA for Certification Authority.

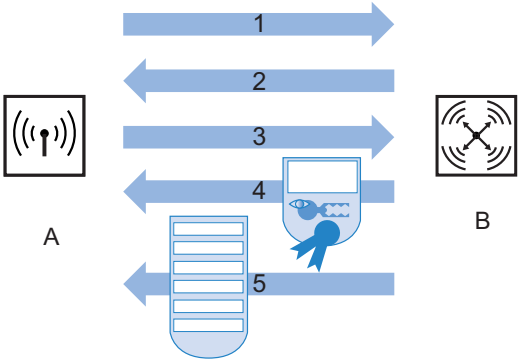


Figure 13: Communication between WLAN Controller and Access Point
A: Access Point
B: WLAN Controller
1: DTLS request
2: SCEP configuration
3: SCEP request
4: Certificate
5: Configuration

Perform the authentication and configuration either automatically or exclusively with a corresponding entry of the Access Point's MAC address in the AP table of the WLAN-Controller. If the Access Point's WLAN modules were deactivated at the beginning of the DTLS communication, the WLAN Controller will activate them after successful transfer of the certificate and configuration.
The management and configuration data will then be transferred via the CAPWAP tunnel. The WLAN Client releases the payload data from the Access Point directly into the LAN and transfers them, for example, to the server.

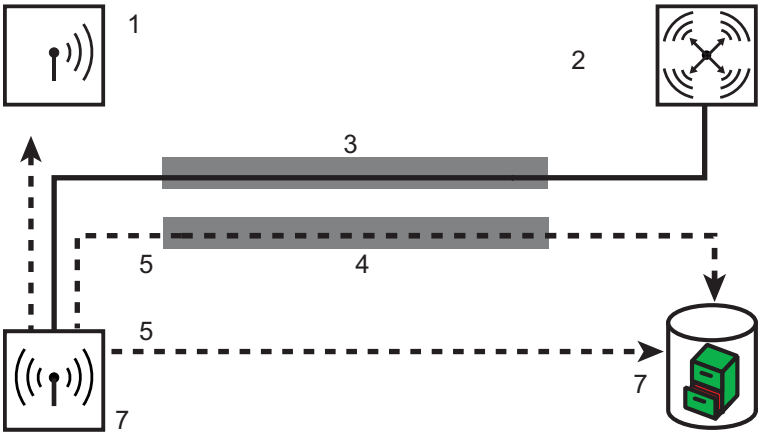


Figure 14: Communication between Access Point and WLAN Controller with CAPWAP tunnel
1: WLAN Client
2: WLAN Controller
3: CAPWAP tunnel
4: CAPWAP tunnel for payload data
5: Payload data
6: Access Point
7: Server

4.2.4 Zero-Touch Management

Hirschmann WLAN Controllers can automatically assign a certificate and configuration to the requesting Access Points. The devices hence implement genuine "zero-touch management". Simply connect new Access Points to the LAN. The Access Points can be operated without special configuration. This simplification to the mere installation of devices reduces the workload of IT departments, especially in decentralized structures. In remote locations, no special IT or WLAN know-how is necessary for the setup.

4.2.5 Split Management

Hirschmann Access Points optionally also locate your WLAN-Controller in remote networks. A simple IP connection, e.g. via a VPN path, is sufficient. As the WLAN-Controllers only influence the WLAN-related part of the configuration in the Access Point, all other functions can be managed separately, if required. Thanks to the distribution of configuration tasks, Hirschmann WLAN Controllers are ideal for setting up a company-wide WLAN infrastructure. The WLAN infrastructure includes the head office and all affiliated branches and home offices.

4.2.6 Inheritance of Parameters

A Hirschmann WLAN-Controller is capable of managing many different Access Points in different locations. The WLAN profile settings are not equally suitable for the managed Access Points. For example, there are differences in the country settings or the device properties.

The logical wireless networks and the physical WLAN parameters can "inherit" specific features from other entries. Even in complex applications, WLAN parameters can thus be managed in common profiles.

- ☐ Initially generate the basic settings that are valid for the majority of managed Access Points.
- ☐ Then generate entries for the more specific values, e.g. country-specific physical settings or a public logical WLAN network.

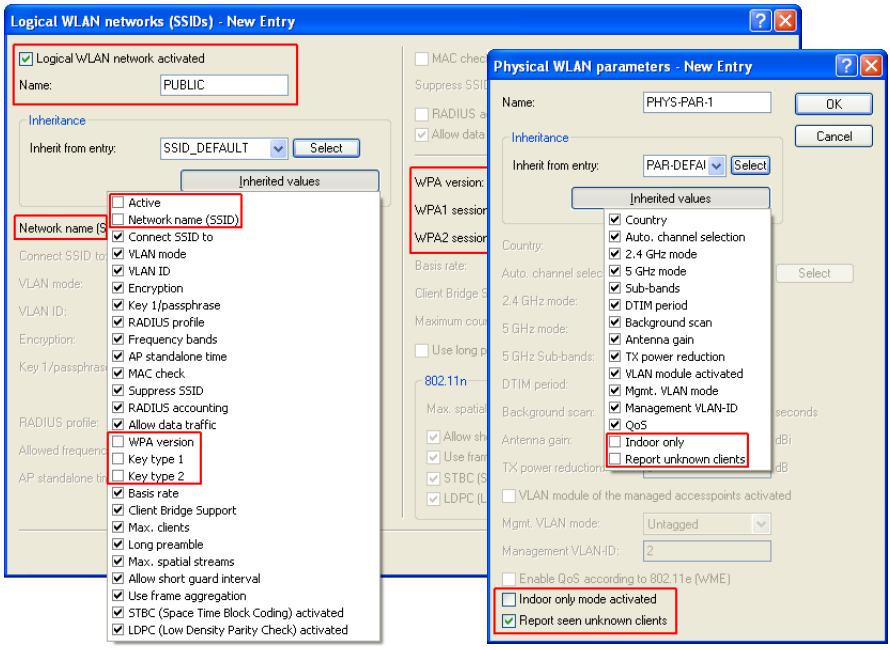


Figure 15: Inheritance of parameters in the case of multiple Access Points

- ☐ Select the entry from which the values are to be inherited and mark the values for inheritance. In the configuration dialog, the inherited parameters will be displayed in gray. You cannot edit these entries.
- ☐ Depending on the application, the edited WLAN settings are then grouped into separate profiles which the device assigns to the respective Access Points.

Note: Inheritance allows chains over multiple stages (cascading). This means that, e.g. country and device-specific parameters can be grouped. Use recursion, if necessary. Profile A then inherits properties from profile B, and at the same time profile B also inherits from profile A. However, the parameters available for inheritance are limited to one "inheritance direction" per parameter.

4.3 Configuration of the WLC

4.3.1 General settings

Most parameters for the configuration of the Hirschmann WLAN Controllers correspond to those of the Access Points. This section describes merely those aspects required for the operation of the WLAN-Controller.
This is where you perform the basic settings for your WLAN-Controller.

☐ Automatically accept new APs (auto-accept)
This option enables the WLAN-Controller to assign a configuration to Access Points without valid certificates as well.
It enables the WLAN-Controller to assign a certificate to all new Access Points without such a valid certificate. One of the following conditions must be fulfilled:
- For the Access Point, a configuration must be entered under its MAC address in the AP table.
- The option 'Automatically provide APs with a default configuration' is activated.

☐ Automatically provide APs with a default configuration
This option enables the WLAN-Controller to assign a default configuration to new Access Points without valid certificates. The WLAN-Controller uses the default configuration for all Access Points for which you do not define an explicit configuration. Together with the auto-accept option, this option permits the automatic acceptance of all Access Points found in the LAN. This automatic process ends as soon as the number of logged-in Access Points reaches the maximum number for the WLAN-Controller. Access Points accepted by default will also appear in the MAC list.

Note: This option might also allow unknown Access Points to access your WLAN structure. Therefore only activate this option during the start-up phase when setting up a centrally managed WLAN structure.
The combination of the settings for auto-accept and the default configuration makes it possible to set up and operate Access Points in different situations:

Auto-accept	Default configuration	Suitable for
On	On	Roll-out phase: Use this combination only if unwanted Access Points cannot be connected to the LAN.
On	Off	Controlled roll-out phase: Use this combination if the following conditions apply: You have entered all approved Access Points along with their MAC address into the AP table. You want to accept the entered Access Points automatically into the WLAN structure.
Off	Off	Normal operation: New Access Points require the administrators' approval to access the WLAN structure.

4.3.2 Profiles

In the profiles area, you define the logical WLAN networks, physical WLAN parameters, and the WLAN profiles which represent a combination of these two elements.

- **WLAN Profiles**
  The WLAN profiles summarize the settings to be assigned to the Access Points. The WLAN profiles are allocated to the Access Points in the AP table.
  For every WLAN profile, define the following parameters:

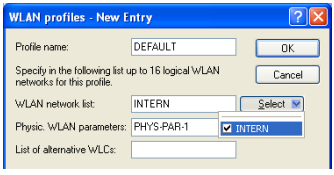


Figure 16: Creating a new WLAN profile

LANconfig: WLAN-Controller > Profiles > WLAN profiles

WEBconfig: HiLCOS-Menu tree > Setup > WLAN management > AP configuration > Common profiles

- ☐ Profile name
  Name of the profile under which the settings are saved.
- ☐ WLAN network list
  List of the logical WLAN networks that are assigned via this profile.
- ☐ Physical WLAN Parameters
  A set of physical parameters that the WLAN modules of the Access Points work with.
- ☐ IP address of alternative WLAN-Controller
  A list of WLAN-Controllers that the Access Point attempts to connect with. The Access Point starts searching for a WLAN-Controller via a broadcast. When the Access Point cannot reach all WLAN-Controllers with such a broadcast, the definition of alternative WLAN-Controllers is advisable. This is the case e.g. when the WLAN-Controller is located in another network.

Logical WLAN Networks

Here you define the logical WLAN networks that the WLAN-Controller assigns to the Access Points. For every logical WLAN network, define the following parameters:

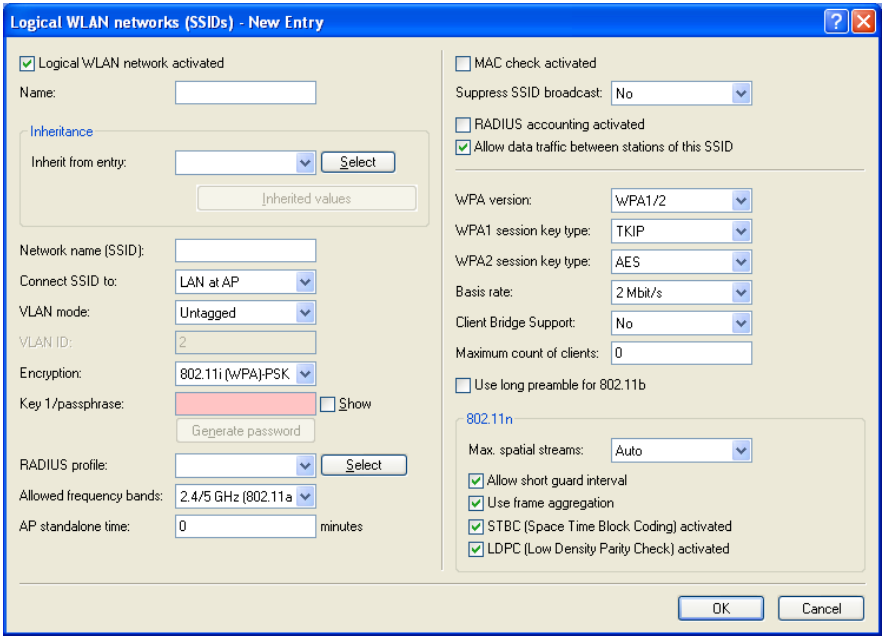


Figure 17: Creating a new entry for a logical WLAN network

LANconfig: WLAN-Controller > Profiles > Logical WLAN networks
WEBconfig: HiLCOS-Menu tree > Setup > WLAN management > AP configuration > Network profiles

☐ Name
Name of the logical WLAN network. This name is only used for the internal management of logical networks.

☐ Inheritance
Selection of a logical WLAN network defined earlier and from which the device inherits the settings.

☐ Network name (SSID):
Service Set Identifier – under this name, the WLAN-Controller propagates the logical WLAN network for the WLAN Clients.

☐ VLAN-ID
VLAN ID for this logical WLAN network.

Note: The use of VLAN IDs in a logical WLAN network requires a management VLAN ID to be set.

☐ Stand-alone operation
Time in minutes that the Access Point continues to operate in its current configuration in managed mode.
The WLAN-Controller transmits the configuration to the Access Point, which optionally stores it in flash memory. This memory area is not accessible to LANconfig or other tools. If the connection to the WLAN-Controller is interrupted, the Access Point will continue to operate with the internal configuration stored in flash memory for the set time period. Even after a local power outage, the Access Point continues to work with this flash configuration.
If there is still no new connection to the WLAN-Controller after the set time period has expired, the Access Point deletes the flash configuration and goes out of operation. As soon as the WLAN-Controller can be reached again, the Access Point transmits the configuration again from the WLAN-Controller to the Access Point. This option enables the Access Point to continue operating even if the connection to the WLAN-Controller is temporarily interrupted. Furthermore this represents an effective measure against data theft as the device automatically deletes all security-related configuration parameters after the set time has expired.

Note: When, in the backup case, the Access Point establishes a connection to a secondary WLAN-Controller, the time for stand-alone operation is paused. The Access Point thus remains active with its WLAN networks even beyond the set time, as long as it is connected to a WLAN-Controller.

Note: The device deletes the configuration data in flash only after the time set for stand-alone operation has run up. When the device is cut off from the power grid, however, the configuration remains in flash memory.

Note: All other parameters of the WLAN networks correspond to those of the standard Access Point configurations.

Physical WLAN Parameters

Here you define the physical WLAN parameters that the WLAN Controller assigns to the Access Points. For every set of physical WLAN parameters, define the following parameters:

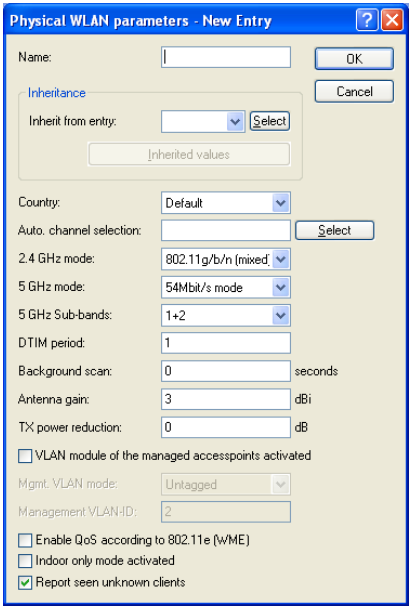


Figure 18: Creating a new entry for a physical WLAN network

LANconfig: WLAN-Controller > Profiles > Physical WLAN parameters
WEBconfig: HiLCOS menu tree > Setup > WLAN management > AP configuration > Radio profiles

- ☐ Name
  Unique name for this combination of physical WLAN parameters.
- ☐ Inheritance
  Selection of a set of physical WLAN parameters defined earlier and from which the entry inherits the settings.
- ☐ Country
  Country in which you operate the Access Points. The device uses this information to define country-specific settings, such as the permitted channels, etc.

- ☐ Automatic channel selection
  By default, the Access Points can use all channels permitted by the country settings. To limit the selection to certain channels, define the desired channels here as a comma-separated list. Ranges can also be defined (e.g. '1,6,11').
- ☐ Management-VLAN ID
  The VLAN ID employed by the management network of the Access Points.

Note: Set the management VLAN ID to a different value than 0 to activate VLANs on the WLAN networks. This also applies when the management network itself is tagged without VLAN IDs (Mgmt-VLAN-ID = 1).
The VLAN activation only applies to those WLAN networks that are connected by means of these physical WLAN parameters.
All other physical WLAN parameters correspond to those for the standard configuration of Access Points.

4.3.3 List of Access Points

- **Access-point Table**
  The AP table is a central element for the configuration of WLAN-Controllers. Here the device transmits a WLAN profile to the Access Points based on their MAC addresses, thus a combination of logical and physical WLAN parameters. Furthermore, the mere existence of an entry for a specific Access Point in the AP table enables it to establish a connection to a WLAN-Controller. For every Access Point, define the following parameters:

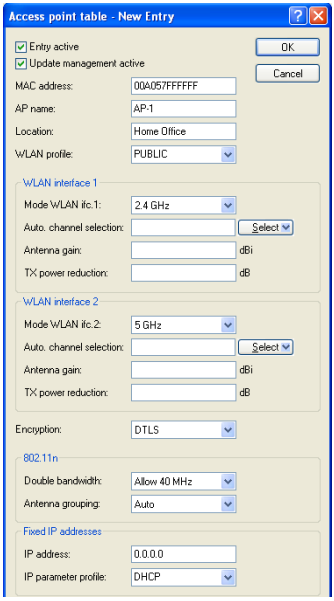


Figure 19: Creating a new Access Point

LANconfig: WLAN-Controller > AP config. > Access-point table
WEBconfig: HiLCOS menu tree > Setup > WLAN management > AP configuration > Access Points

- ☐ Update management active
  Activating update management enables the Access Point to automatically upload the latest firmware or script versions. All other settings are made under AP update.
- ☐ MAC address
  MAC address of the Access Point.
- ☐ Exclusive AP name
  Name of the Access Point in managed mode.
- ☐ Location
  Location of the Access Point in managed mode.
- ☐ WLAN profile
  WLAN profile from the list of defined profiles
- ☐ WLAN interface 1
  Frequency band for the 1st WLAN module. Use this parameter to optionally deactivate the WLAN module.

- ☐ Auto. channel selection Ifc 1
  If no entry is made here, Access Points automatically carry out the channel selection for the frequency band available in the set country of operation.
  Enter the channels to which the automatic selection will be restricted for the first WLAN module. If you enter exactly one channel, the device will use this channel exclusively. In such a case there will be no automatic selection. Therefore when entering a channel number, be certain that it is really valid in the frequency band of the respective country. The device ignores channels that are invalid for the defined frequency band.
- ☐ WLAN interface 1
  Frequency band for the 1st WLAN module. Use this parameter to optionally deactivate the WLAN module.
- ☐ WLAN interface 2
  Frequency band for the 2nd WLAN module.
- ☐ Auto. channel selection Ifc 2
  Automatic channel selection for the 2nd WLAN module.

Note: The device ignores the settings for the second WLAN module, if the managed device has only one WLAN module.

- ☐ Encryption
  Here you define the encryption for the communication over the control channel. Without encryption, the devices exchange the control data as plain text. In both cases authentication is based on certificates.
- ☐ Double bandwidth
  For Hirschmann Access Points according to IEEE 802.11n, activate the use of the double bandwidth here.
- ☐ Antenna grouping
  To optimize the gain through spatial multiplexing, configure the antenna grouping here.
- ☐ IP address
  Specify the static IP address of the Access Point here.
- ☐ IP parameter profile
  Enter the profile name here which the device uses to reference the IP settings for the Access Point. If you retain the default setting DHCP, the Access Point ignores the setting for the static IP address and retrieves its IP address via DHCP.

Default Parameters

You can define central default values for some parameters which the device references as 'default' in other parts of the configuration (for example, using the "Access point table".

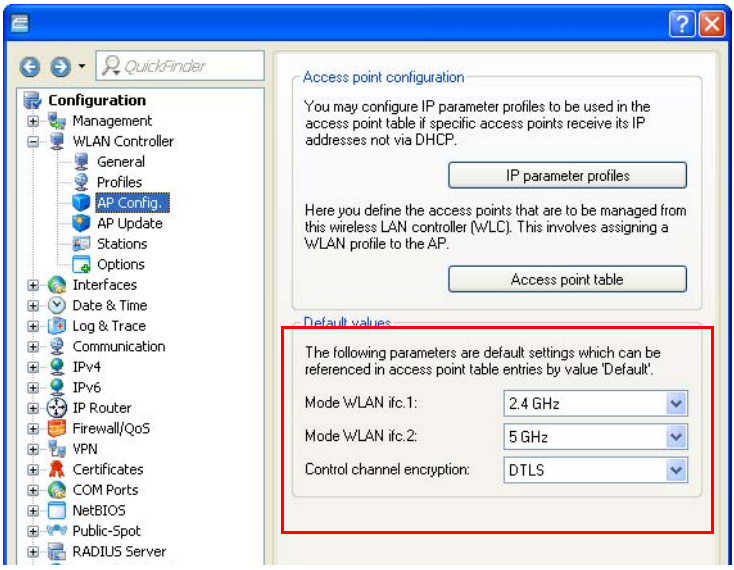


Figure 20: Defining central default values

LANconfig: WLAN-Controller > AP config. > Default values
WEBconfig: HiLCOS-Menu tree > Setup > WLAN management > AP configuration

☐ WLAN interface 1
Frequency band for the 1st WLAN module. Use this parameter to optionally deactivate the WLAN module.

☐ WLAN interface 2
Frequency band for the 2nd WLAN module. Use this parameter to optionally deactivate the WLAN module.

☐ Encryption
Encryption for the communication over the control channel. Without encryption, the devices exchange the control data as plain text. In both cases authentication is based on certificates.

4.3.4 Station Table (ACL Table)

By means of the station table, you define which WLAN Clients can access the WLAN networks of the managed Access Point. Furthermore, the method offers a convenient way to assign an individual authentication passphrase and a VLAN ID to each WLAN Client.
It is imperative that the RADIUS server in the WLAN-Controller is activated in order to use the station table. As an alternative, requests can be forwarded to another RADIUS server.
Activate the MAC check for every logical WLAN network in which WLAN Clients are authenticated by RADIUS.

4.3.5 Options for the WLAN-Controller

In the 'Options' area, you can define notifications in case of events in the WLAN-Controller and set various default values.

Notification can take place via SYSLOG or e-mail. Define the following parameters:

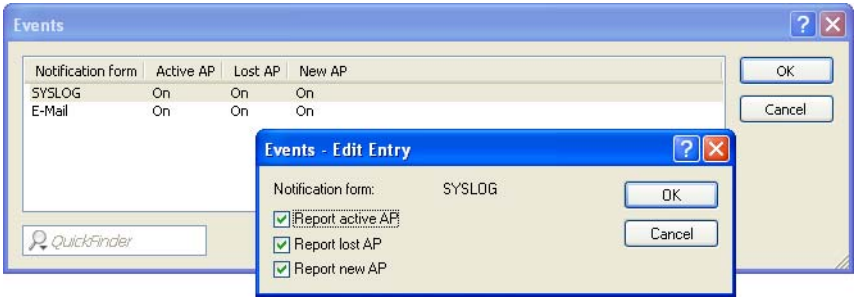


Figure 21: Setting a new event notification

LANconfig: WLAN-Controller > Options > Events
WEBconfig: HiLCOS-Menu tree > Setup > WLAN management > Event notification

- SYSLOG
  Activates notification via SYSLOG.
  Possible values: On/Off.
- E-mail
  Activates notification via e-mail.
  Possible values: On/Off.
- Events
  Selects the events that trigger a notification.
  Possible values:
  - Active Access Point notification
  - Missing Access Point notification
  - New Access Point notification

4.4 Configuring the Access Points

By default, the WLAN modules in the Access Points are set to the operating mode 'Access Point'. In this mode, the devices function as stand-alone Access Points and use a configuration that is stored locally in the device. Switch the operating mode for the WLAN modules in the desired Access Points to 'managed' to integrate them into a centrally managed WLAN structure.

Note: You can define the operating mode separately for every WLAN module. For models with 2 WLAN modules, depending on the application, one module can work with a local configuration, the 2nd module can be part of a centrally managed WLAN structure.

For individual devices, the operating mode of the WLAN modules can be found in LANconfig under Wireless LAN > General > Physical WLAN settings > Operation mode:

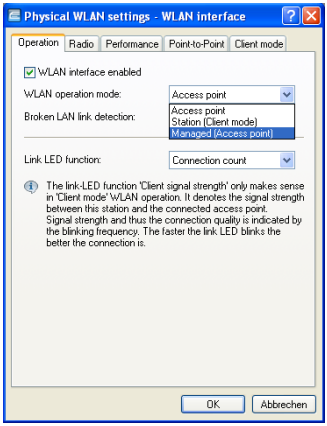

Physical WLAN settings - WLAN interface
Operation
Radio
Performance
Point-to-Point
Client mode
WLAN interface enabled
WLAN operation mode:
Access point
Broken LAN link detection:
Access point
Station (Client mode)
Managed (Access point)
Link LED function:
Connection count
The link-LED function 'Client signal strength' only makes sense in 'Client mode' WLAN operation. It denotes the signal strength between this station and the connected access point. Signal strength and thus the connection quality is indicated by the blinking frequency. The faster the link LED blinks the better the connection is.
OK
Abbrechen

Figure 22: Changing the operating mode of the Access Points to 'managed'

To change the operating mode for multiple devices at the same time, start a simple script for the devices with the following lines:

```
# Script (7.22 / 23.08.2007
lang English
flash 0
cd Setup/Interfaces/WLAN/Operational
set WLAN-1 0 managed-AP 0
# done
exit
```

4.4.1 WLAN band steering

The IEEE 802.11 standard contains virtually no criteria by which a WLAN client should select the access point. While there are general guidelines according to which preference is given to an access point with a higher RSSI value (i.e. the received signal strength), for example, WLAN clients do not, in practice, adhere strictly to these definitions or the general guidelines. If both 2.4GHz and 5GHz are used to broadcast an SSID, there is normally no way of influencing the client as regards the preferred frequency band.

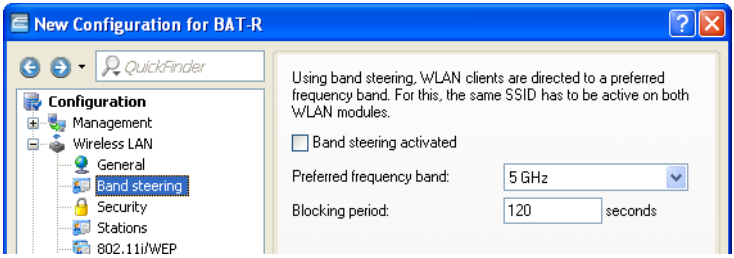
The steering of WLAN clients is based on the principle that many clients determine the available access points by means of an active scan. Active scanning here means that a client sends probe requests containing the network ID to which the client is to connect. Access points with this ID then send a test response, enabling the client to create a list of available access points. The vast majority of WLAN clients only connect to access points from which they have received a probe response, and this can be used to steer their selection process.

There are multiple, sometimes very advanced, criteria for steering. One of these criteria relates to the wireless frequency ranges used for client communication. Modern dual-band WLAN clients are expected to prefer the 5GHz frequency band over the (now) overcrowded 2.4GHz band. Band steering is the term given to purposefully assigning a WLAN client a particular frequency band or range.

The list of detected or "seen" clients contains all clients from which the access point has received a test request packet. In combination with the radio frequency on which the WLAN client sends the test request, this list is one of the bases on which the access point decides whether to respond to the request or not.

Other criteria depend on the reported client IDs and the configuration of the devices. It may be the case, for example, that fewer SSIDs are reported on the preferred frequency band than are on the one with the lower preference. Similarly, too low a transmit strength when SSIDs are reported can result in the client not receiving any probe responses at all on the preferred frequency band. For the latter scenario, it is important to ensure that the access point does not suppress probe responses on the less favored frequency band. This is controlled by the setting for minimum signal strength, which you set in LANconfg under `Wireless LAN:General:Logical WLAN settings:Network: Minimum client signal strength`.

The band steering of the access point itself is enabled and managed in LANconfig under `Wireless LAN:Band steering`.



In this window you have the following options:

- **Band steering activated**: Activates or deactivates this function.
- : Specifies the frequency band to which the device steers WLAN clients. Possible values are:
  - **2.4GHz**: The device routes clients to frequency band 2.4GHz.
  - **5GHz**: The device routes clients to frequency band 5GHz.
- **Blocking period**: The time for which the access point steers the WLAN client to the preferred frequency band. The default value is 120 seconds.

4.4.2 UUID Information Element for WLAN Access Points

Current Hirschmann devices are multi-SSID capable, i.e. you can simultaneously present different 'virtual' access points to multiple WLAN clients.

For devices with two radio modules (dual radio), the BSSIDs relate to the logical networks on the corresponding radio module. However, the MAC addresses of the two radio modules are completely independent of one another. Consequently, logical networks with different BSSIDs cannot be unequivocally related to a single device.

However, for the planning and monitoring of networks, it is often desirable to be able to relate logical networks to their respective devices (or radio modules).

The access points support an Aironet-compatible information element that contains the name of the device as assigned to it by the administrator. The transmission of this information is optional and many operators disable it for security reasons because they want to publish as little information as possible about the access point on the network.

Thus, this information either does not appear for network monitoring at all or, depending on the setting, the information may not identify the device as an access point.

Besides this, the access points possess a UUID (universally unique identifier), which is calculated from the device type and serial number and can identify the device uniquely on the network. By using encryption when generating the UUID, the device type or serial number can only be inferred with considerable effort (brute-force attack for all types of devices and serial numbers).

Transmission of the Aironet-compatible information element and of the UUID can be switched on or off independent of the radio module and logical network. This is done in the WEBconfig under

```
HiLCOS Menu Tree:Setup:Interfaces:WLAN:Network:Aironet-
Extensions
HiLCOS Menu Tree:Setup:Interfaces:WLAN:Network:Include-UUID
```

4.4.3 PMK Caching in the WLAN Client Mode

When establishing a connection from a WLAN client to an access point operating with 802.1x-authentication, the two stations negotiate a shared key, known as the Pairwise Master Key (PMK), for the subsequent encryption. In applications with mobile WLAN clients (laptops in large offices, moving objects with WLAN connections in the industrial sector), the WLAN clients often change the access points via which they are logged in to the WLAN network. And although WLAN clients roam back and forth between different access points, in most cases these tend to be the same ones.

Access points typically save a negotiated PMK for a certain period of time. WLAN devices in WLAN client mode also store PMKs. As soon as a WLAN client starts to login to an access point that it was previously connected to, the WLAN client can directly transfer the existing PMK to the access point. In this way, the two remote stations skip the PMK negotiation phase while establishing the connection, and the WLAN client and access point establish the connection much faster.

The WLAN client stores the negotiated PMK for the duration set under `Default lifetime`.

`HiLCOS Menu Tree:Setup:WLAN:PMK-Caching:Default-Lifetime`

4.4.4 Pre-authentication in WLAN Client Mode

Fast authentication by means of the Pairwise Master Key (PMK) only works if the WLAN client was logged on to the access point previously. The WLAN client uses pre-authentication to reduce the time to logon to the access point at the first logon attempt.

`HiLCOS Menu Tree:Setup:WLAN:Encryption:Pre-authentication`

Usually, a WLAN client carries out a background scan of the environment to find existing access points that it could connect to. Access points that support WPA2/802.1x can communicate their pre-authentication capability to any WLAN clients that issue requests. A WPA2 pre-authentication differs from a normal 802.1x authentication as follows:

- The WLAN client logs on to the new access point via the infrastructure network, which interconnects the access points. This can be an Ethernet link, a WDS link (wireless distribution system), or a combination of both.
- A pre-authentication is distinguished from a normal 802.1x authentication by the differing Ethernet protocol (EtherType). This allows the current access point and all other network partners to treat the pre-authentication as a normal data transmission from the WLAN client.
- After successful pre-authentication, the negotiated PMK is stored to the new access point and the WLAN client.

  Note: The use of PMKs is a prerequisite for pre-authentication. Otherwise, pre-authentication is not possible.

- When the client wants to connect to the new access point, the stored PMK significantly accelerates the logon procedure. The further procedure is equivalent to that described under PMK caching(see page 229).

Note: On the client side, the number of concurrent pre-authentications is limited to four. This minimizes the network load on the central RADIUS server in network environments with large numbers of access points.

4.4.5 Time-staggered Roaming for Dual-radio Client WLAN Modules

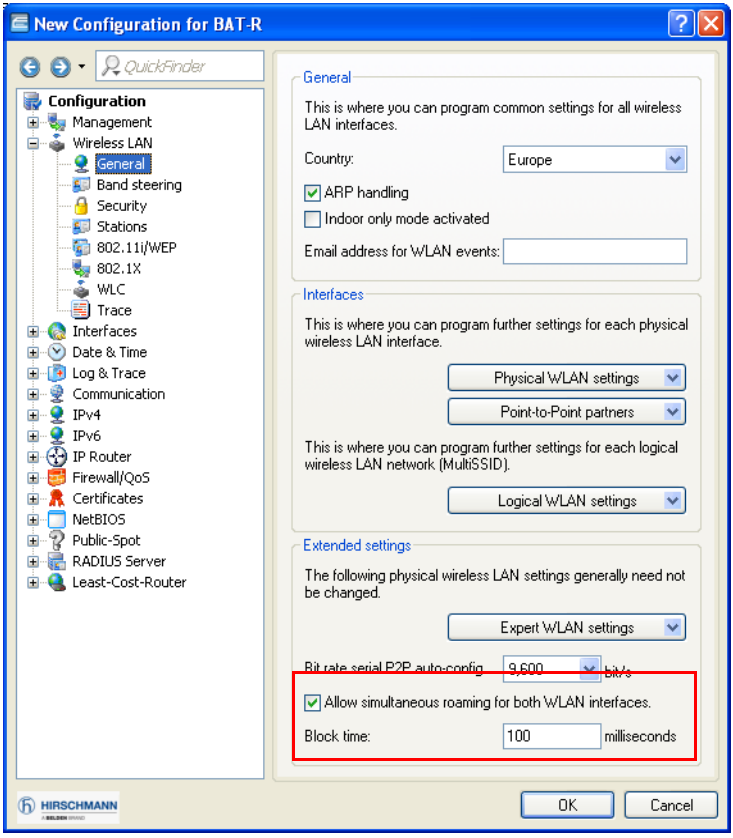
If a dual-radio client moves from a WLAN cell to an adjacent cell, multi-radio handover coordination in the device ensures that a WLAN module remains connected to the current access point until the second WLAN module is successfully logged in to the new WLAN cell.

If this function is enabled and there are one or more WLAN modules in the registration phase, the WLAN client locks the registration of the WLAN module with an existing connection. This prevents both of the modules simultaneously attempting to log in to the new cell, which would cause both WLAN connections to be lost.

If the locked WLAN module loses the data connection before one of the other modules has negotiated a new data connection, the client of this module unlocks it to negotiate a new data connection.

If the WLAN module has successfully logged in to the new WLAN cell, the other module remains connected for a minimum period (the "Block time"), so that the access point of the new cell has enough time to update its network entries. During this minimum period, this module performs no roaming and no background scanning.

Time-staggered roaming is enabled in LANconfig under `Wireless LAN:General:Extended settings:Allow simultaneous roaming for both WLAN interfaces`.



4.4.6 Greenfield Mode for Access Points with IEEE 802.11n

For access points that comply with the IEEE 802.11n standard, the physical WLAN settings provide the option to allow or restrict data transmission according to the IEEE 802.11n standard.

The IEEE 802.11n standard only allows data links that are either encrypted with WPA2/AES or unencrypted. WEP- and TKIP-based encryptions are not allowed in IEEE 802 11n. Please be aware of the following restrictions depending on the actual physical and logical WLAN settings:

Along with the selection of the individual a/b/g/n standards and a selection of mixed operating modes, the access points provide the option of using the Greenfield mode. Once activated in the physical WLAN settings for a WLAN interface, the Greenfield mode only allows WLAN clients that support the IEEE 802.11n standard to associate with the corresponding logical WLANs (SSIDs). Other WLAN clients that only work with the standards IEEE 802.11a/b/g cannot associate with these WLANs. In LANconfig, you activate the "Greenfield Mode" in the menu `Wireless LAN:General: Physical-WLAN-Settings:Radio:2.4-GHz mode`.

- If, in the Physical settings, you activate support of a mixed-mode which includes the IEEE 802.11n standard and individual WLAN clients on a logical network support WEP encryption only, then the access point will reduce the transmission rate to the 802.11a/b/g standard, because the higher transfer rates available with IEEE 802.11n are not supported in combination with WEP.
- If, in the Encryption settings for a logical WLAN network, you enable not only AES session keys but also TKIP session keys, then the access point will use only the AES session key for this WLAN, because TKIP is not supported by IEEE 802.11n.
- If, in the Encryption settings for a logical WLAN network, you enable only TKIP session keys, then the access point will reduce the transmission rate to the 802.11a/b/g standard, because the higher transfer rates available with IEEE 802.11n are not supported in combination with TKIP.

4.5 Related Information on General WLAN Configuration

4.5.1 STBC / LDPC

Basics

Data transfers according to the IEEE-802.11n standard are performed using MIMO technology (multiple input, multiple output). The sender transmits data packets concurrently over multiple, spatially separated antennas, meaning that reflections and the resulting interference have little effect on the signal. However, the gain in throughput is less with each additional antenna, and the performance requirements for signal processing are increased.

Low Density Parity Check (LDPC)

Before the sender transmits the data packets, it expands the data stream with checksum bits depending on the modulation rate. These checksum bits allow the receiver to correct transmission errors. By default the 802.11n standard uses 'Convolution Coding' (CC) for error correction, which is well-known from the 802.11a and 802.11g standards; however, the 11n standard also provides for error correction according to the LDPC method (Low Density Parity Check).

In contrast to CC encoding, LDPC encoding uses larger packets to calculate checksums and can also recognize more bit errors. The improved ratio of payload to checksum data enables LDPC encoding to provide a higher data transfer rate.

Space Time Block Coding (STBC)

The function 'STBC' (Space Time Block coding) additionally varies the transmission of data packets over time to minimize time-related effects on the data. Due to the time offset of the packets the recipient has an even better chance of receiving error-free data packets, regardless of the number of antennas.

4.5.2 DFS

As of HiLCOS version 8.80 all devices transmitting on the 5GHz WLAN frequencies support the standard ETSI EN 301 893 V1. 6. 1 ("DFS4").

Function and the History of Development

For the DFS method (Dynamic Frequency Selection) required for 5 GHz WLANs, an unused frequency is automatically selected, for example, to avoid interference from radar systems. Occasionally, however, signals from weather radar stations cannot be identified reliably.

For this reason the European Commission is extending the requirements of the standards ETSI EN 301 893 V1.3.1 and ETSI EN 301 893 V1.4.1 to additionally avoid the use of three channels (120, 124 and 128) in subband 2 of the 5 GHz band. The use of these bands for automatic channel selection is prohibited until a process to auto-detect weather radar station signals becomes available. The versions EN 301 893 V1.3 and EN 301 893 V1.4 are referred to as "DFS2"

In the middle of 2010 the new version ETSI EN 301 893 V1.5.1 came into force, which was accompanied by changes in the usage of WLAN frequencies in the ranges 5.25 to 5.35 GHz and 5.47 to 5.725 GHz. The new Version 1.5.1 regulates the DFS (Dynamic Frequency Selection) method for the protection of radar stations from WLAN systems working

in this frequency range. By using DFS to detect certain patterns in the radio signals received, it is now possible to detect active radar stations, and WLAN systems can automatically switch their operating channel. To differentiate from previous regulations, the new standard EN 301 893-V1.5 for the updated DFS is referred to as "DFS3".

A pulse pattern can generally be described in terms of its pulse rate, pulse width and the number of pulses. Former DFS technology was only able to detect fixed radar patterns as defined by the various combinations of pulse rates and pulse widths which were stored in the WLAN device. According to DFS3, the device is now able to recognize changing pulse rates and pulse widths as radar patterns. Furthermore, two or three different pulse rates may be used within a radar signal.

The version ETSI EN 301 893 V1.5.1 (DFS-3) expires on 01/01/2013. The new version ETSI EN 301 893 v1.6.1 (known as "DFS4"), which also detects shorter radar pulses, applies thereafter.

Note: The recognition of weather radar stations (channels 120, 124 and 128 in the 5.6 to 5.65 MHz frequency range) is subject to special conditions. The DFS implementation in HiLCOS does not support the more stringent recognition conditions. Therefore, these three channels will be omitted from newer versions of HiLCOS.

4.6 Managing the Access Points

4.6.1 Accepting new Access Points manually into the WLAN structure

To integrate the Access Points into the WLAN structure without the automatic (auto-accept) option, accept the Access Points manually.

- Access PointAccepting Access Points via LANmonitor
  You can accept new Access Points comfortably via the LANmonitor. Select a configuration that the Access Point uses after transmission of a new certificate.
  In LANmonitor, click the new Access Point with the right-hand mouse button to integrate it into the WLAN structure. From the context menu that pops up, select the configuration for the device.

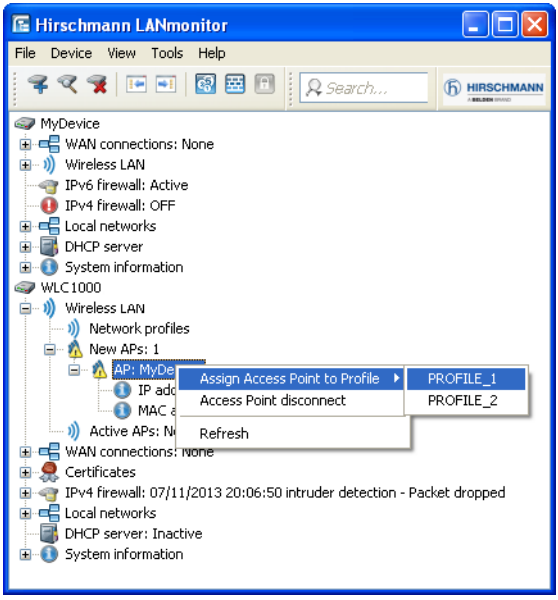


Figure 23: Accepting new Access Point via LANmonitor

Note: This process defines the Access Point in the AP table of the WLAN-Controller. As soon as the Access Point has built up the random, the WLAN-Controller assigns a certificate to the Access Point. Only then will the Access Point become an active element of the central WLAN structure. Until assignment of the certificate is completed, the WLAN-Controller reports the new Access Point with the red Lost-AP LED in the device display and as "Lost AP" in the LANmonitor.

Access PointAccepting Access Points via WEBconfig with Assignment of a Certificate

New Access Points with entry in the AP table but without valid certificate can be accepted manually via an action in WEBconfig.

- ☐ Open the configuration of the Hirschmann WLAN-Controller with WEBconfig.
- ☐ Under HiLCOS menu tree>Setup > WLAN management, select the action Accept AP.
- ☐ As parameter for the action, transmit the MAC address of the Access Point that you are integrating into the WLAN structure. Confirm the action with "Execute".

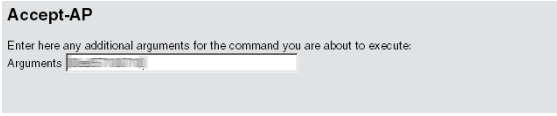


Figure 24: Accepting a new Access Point via WEBconfig with assignment of a certificate

- **Access PointAccepting Access Points via WEBconfig with Assignment of a Certificate and Configuration**
  New Access Points without entry in the AP table and without valid certificate can be accepted via a new wizard in WEBconfig. Define a configuration that the Access Point uses after transmission of a new certificate.
  - ☐ Open the configuration of the Hirschmann WLAN-Controller with WEBconfig. Among the setup wizards, select the wizard "Assigning new Access Points to profiles".

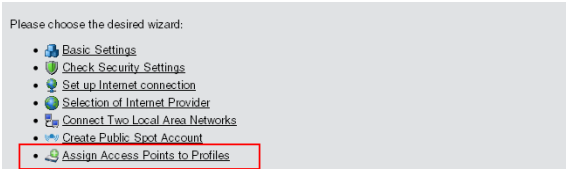

Please choose the desired wizard:
Basic Settings
Check Security Settings
Set up Internet connection
Selection of Internet Provider
Connect Two Local Area Networks
Create Public Spot Account
Assign Access Points to Profiles

Figure 25: Accepting a new Access Point via WEBconfig with assignment of a certificate and configuration

  - ☐ Click the link to start the wizard. Select the desired Access Point based on its MAC address and enter the WLAN configuration that the device shall assign to the Access Point.

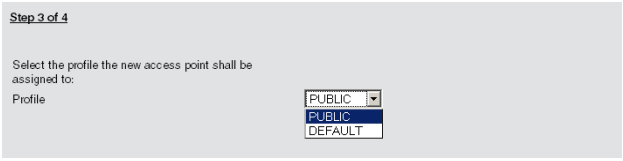


Figure 26: Selecting the WLAN configuration

Note: With the assignment of the configuration, the WLAN-Controller integrates the selected Access Point into the AP table. As soon as the Access Point has built up the random, the WLAN-Controller assigns a certificate to the Access Point. Only then will the Access Point become an active element of the central WLAN structure. Until assignment of the certificate is complete, the WLAN-Controller reports the new Access Point with the red Lost-AP LED in the device display and as "Lost AP" in the LANmonitor.

4.6.2 Removing Access Points manually from the WLAN structure

Perform the following actions to remove a managed Access Point from the WLAN structure:

- ☐ In the Access Point, switch the WLAN operating mode for the WLAN modules from 'managed' to 'client' or 'Access Point'.
- ☐ In the WLAN-Controller, delete the configuration for the Access Point or deactivate the option 'automatic assignment of the default configuration'.
- ☐ Disconnect the Access Point in WEBconfig under HiLCOS menu tree > Setup > WLAN management with the action 'disconnect AP connection' or alternatively in LANmonitor.
- ☐ As parameter for the action, transmit the MAC address of the Access Point that you are removing from the WLAN structure. Confirm the action with "Execute".

Figure 27: Manually removing an Access Point from the WLAN structure

4.6.3 Deactivating or Permanently Removing Access Points from the WLAN Structure

In some cases it is necessary to temporarily deactivate or permanently remove an Access Point managed by the WLAN-Controller.

- **Access Point Deactivating Access Points**
  To deactivate an Access Point, set the corresponding entry in the AP table to 'inactive' or delete the entry from the table. This process deactivates the WLAN modules in managed mode and deletes the corresponding SSIDs in the Access Point.

  Note: This process deactivates the WLAN modules and the WLAN networks (SSIDs) even if stand-alone operation is activated.

  An Access Point deactivated like that remains connected to the WLAN-Controller, the certificates are retained. The WLAN-Controller activates the Access Point and its WLAN modules in managed mode, if required. It can do this by activating the existing entry or creating a new entry for the corresponding MAC address in the AP table.

- **Access Point Permanently Removing Access Points from the WLAN Structure**
  Delete or cancel the certificates in the SCEP client to permanently remove an Access Point from the centrally managed WLAN structure.
  - ☐ If you have access to the Access Point, delete the certificates by resetting the device.
  - ☐ If a device has been stolen and you want to remove it from the WLAN structure, cancel the certificates in the CA of the WLAN-Controller. In WEBconfig, go to the area Status > Certificates > SCEP-CA > Certificates and access the Certificate status table. Delete the certificate for the MAC address of the respective Access Point here. The certificates are marked as expired, but remain in the device.

  Note: In case of a backup solution with redundant WLAN-Controller, cancel the certificates in all WLAN-Controllers.

4.6.4 Managing the Access Points

LANmonitor gives you a quick overview of the Hirschmann WLAN-Controllers in the network and the Access Points within the WLAN structure. LANmonitor LANmonitor displays the following information, among others:

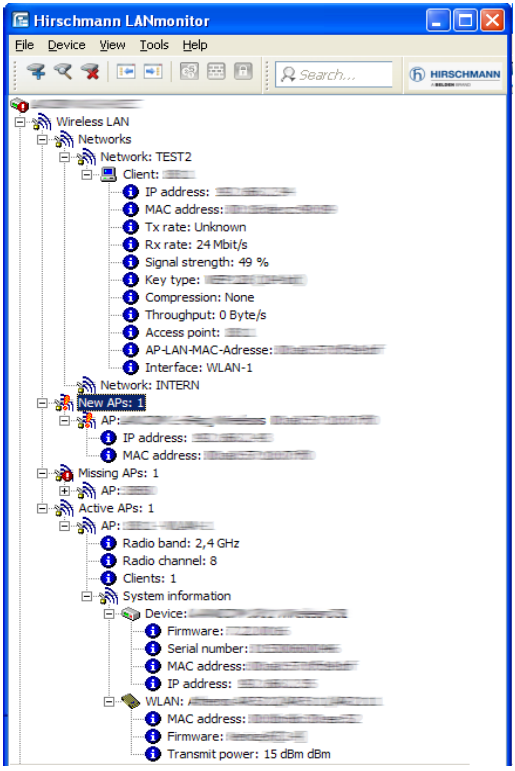


Figure 28: Network in LANmonitor

- ☐ Active WLAN networks with logged-in WLAN Clients and the name of the Access Point where the WLAN Client is logged in.
- ☐ Display of new Access Points with IP and MAC address

- ☐ Display of missing Access Points with IP and MAC address
- ☐ Display of managed Access Points with IP and MAC address, utilized frequency band and channel

Use the right-hand mouse button while pointing at the Access Points to open a context menu with the following actions:

- ☐ Assign new Access Point to profile
  This action assigns a configuration to a new Access Point and integrates it into the WLAN structure.
- ☐ Access Point Disconnect Access Point
  Disconnects Access Point and WLAN-Controller. The Access Point then carries out a new search for the responsible WLAN-Controller. Use this action, e.g., after a backup event to disconnect Access Points from the backup controller and to redirect them to the actual WLAN-Controller.
- ☐ Refresh
  Refreshes the display of the LANmonitor.

4.6.5 Backing up the Certificates

At the first system startup, a Hirschmann WLAN-Controller creates the root certificates for the CA (Certification Authority) and the RA (Registration Authority). Based on these two certificates, the WLAN-Controller generates the device certificates for the Access Points.
Use the same root certificates in the following cases, to ensure smooth operation of the managed Access Points:

- ☐ when you are employing several WLAN-Controllers in parallel within the same WLAN infrastructure (load balancing) or
- ☐ when you are replacing or reconfiguring a device.

Creating Backups of the Certificates

To restore the CA or RA, the device requires the relevant root certificates with the private keys that the WLAN Controller generates automatically at system start. Furthermore back up further files containing information on issued device certificates. To ensure that this confidential information remains protected even when exported from the device, the device initially stores it to a passphrase-protected PCKS12 container.

- ☐ Open the configuration of the Hirschmann WLAN-Controller with WEBconfig under HiLCOS menu tree > Setup > Certificates > SCEP-CA > CA certificates.
- ☐ Select the command "create PKCS12 backup files" and enter the passphrase for the PCKS12 container as parameter.

Create-PKCS12-Backup-Files
Enter here any additional arguments for the command you are about to execute:
Arguments Passphrase

Figure 29: Creating backups of the certificates with PCKS12 container

This action saves the certificates and private keys in PKCS12 files. The files are then available for download from the device.

Downloading Certificate Backups from the Device

- ☐ Select File management > Download certificate or file
- ☐ Then, as file type, select the two entries for the SCEP-CA one after the other and confirm with Start download:
  - ▶ PKCS12 container with CA backup
  - ▶ PKCS12 container with RA backup

Download Certificate or File
Select which file you want to download, then click on 'Start Download':
File Type: SCEP-CA - PKCS12 container with CA backup

Figure 30: Downloading certificate backups from the device

This action saves the backup files to your data carrier. You will not require the passphrase until the backup is uploaded to a Hirschmann WLAN-Controller.

- Uploading a Certificate Backup to the Device
  - ☐ Select File management > Upload certificate or file
  - ☐ Then select the two entries for the SCEP-CA as file type one after the other:
    - ▶ PKCS12 container with CA backup
    - ▶ PKCS12 container with RA backup
  - ☐ For each upload, enter the file name with storage location and the corresponding passphrase. Confirm with Start upload:
  - ☐ After loading the CA backup, delete the file controller_rootcert in the directory /Status/File-System/Contents. Enter the following commands in the console:
    `cd /Status/File-System/Contentsdel controller_rootcert`
  - ☐ Then access the directory /Setup/Certificates/SCEP-Client and execute the command Reinit:
    `cd /Setup/Certificates/SCEP-Clientdo Reinit`

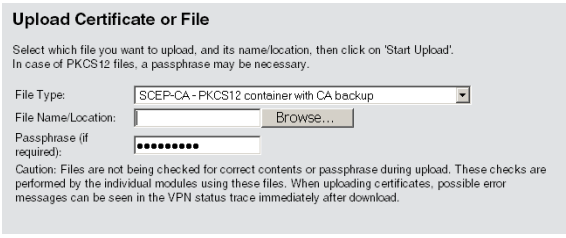

Upload Certificate or File
Select which file you want to upload, and its name/location, then click on 'Start Upload'.
In case of PKCS12 files, a passphrase may be necessary.
File Type:
SCEP-CA - PKCS12 container with CA backup
File Name/Location:
Browse...
Passphrase (if required):
Caution: Files are not being checked for correct contents or passphrase during upload. These checks are performed by the individual modules using these files. When uploading certificates, possible error messages can be seen in the VPN status trace immediately after download.

Figure 31: Uploading a certificate backup onto the device

4.6.6 Saving and Restoring more files of the SCEP-CA

To fully restore the SCEP-CA, the information on the device certificates issued by the SCEP-CA for the individual Access Points is also important.

Note: If you back up only the root certificates, there is no possibility to call up the issued device certificates.

For this reason, back up the following files in addition to the certificates:
- ☐ SCEP certificate list: List of all certificates ever issued by the SCEP-CA.
- ☐ SCEP serial numbers: Contains the serial number for the next certificate.
- ☐ Select File management > Download certificate or file.
- ☐ Then, as file type, select the two entries listed above one after the other and confirm with Start download:

Download Certificate or File
Select which file you want to download, then click on 'Start Download':
File Type:
SCEP-CA - Certificate list

Figure 32: Backing up further files of the SCEP-CA

- ☐ To upload these files to the device, go to the start page of WEBconfig and select the command Upload certificate or file.
- ☐ Then, as file type, select the two entries listed above one after the other, enter each file name and the storage location and confirm with Start upload:

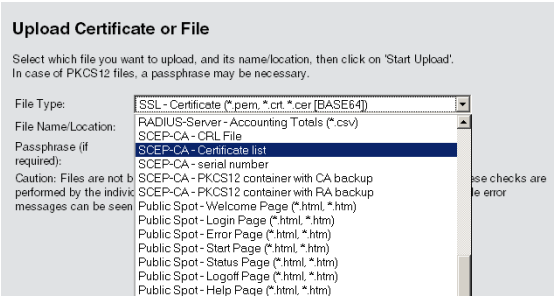


Figure 33: Restoring further files of the SCEP-CA

Note: After a new certificate list has been loaded, the device removes expired certificates and generates a new CRL. Furthermore, the CA reinitializes itself automatically if certificates and keys have been successfully extracted after loading the certificate backup.

4.7 Interference Detection in the Frequency Range (Spectral Scan)

In addition to connecting computers to the Internet, professional users are increasingly using wireless local area networks (WLAN) for business-critical applications. Examples include accessing of patient files, online monitoring of production facilities, and the transmission of video and audio data (ideally without any time lags). The reliability and performance of WLAN systems are thus increasingly important.

The rising significance and usage of WLAN for data transmission is resulting in more and more scenarios where the equipment and systems of various users are crowding the WLAN frequency ranges. These may include, for example, microwave ovens, cordless telephones, Bluetooth devices and video transmitters, with their signals occurring on a continual or intermittent basis. The simultaneous usage of a frequency band or frequency range gives rise to interference that can disrupt or negatively impact the reliability and performance of a WLAN. This type of interference can result in lost data packets or connection failure. If the interference is too strong, the complete failure of the WLAN may result.

It is therefore becoming increasingly important to use targeted analysis to check the frequency ranges. These checks should identify the interference or other interference factors, and introduce countermeasures as required. It can also be used to ensure that the WLAN is working properly and operating interference free.

Targeted analysis can also clarify or identify the following:

- Proper, fault-free operation of the WLAN
- Existence of interference or noise
- Display or identify the bands with interference
- Strength of the interference signal
- Regularity or frequency of the interference signal
- Type, and possibly source, of the interference signal

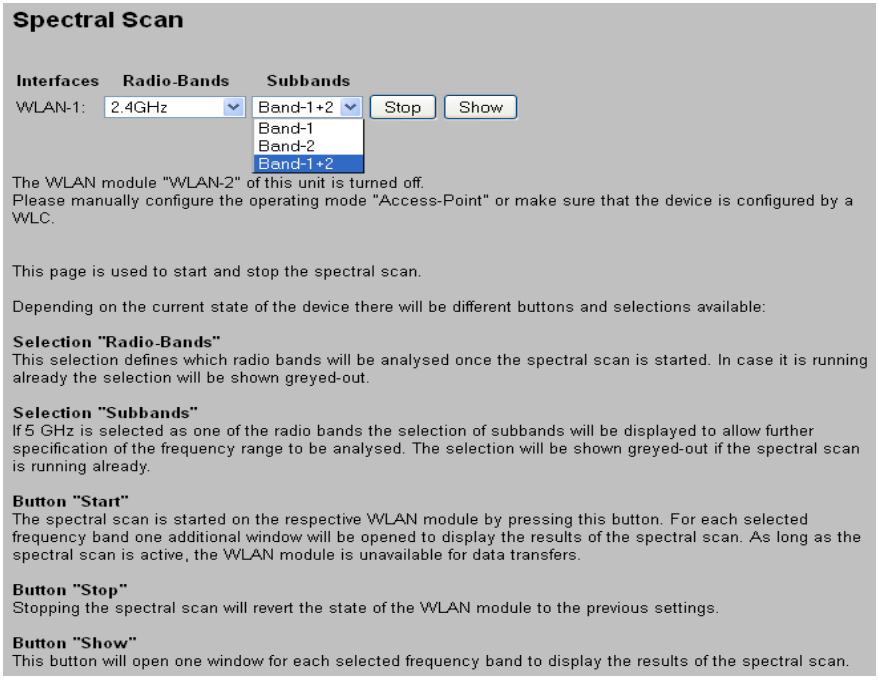
The WLAN-related frequency ranges are subject to spectral analysis. Results are displayed graphically, i.e. in the form of real-time diagrams or real-time overviews of frequencies and interference. However, graphical analyses of a spectral range are open to some freedom of interpretation. Therefore, the following scenario should be fairly commonplace: You ascertain that the frequency currently being used is being subjected to interference that is continual and of constant signal strength. However, you are not able to ascertain unequivocally which room or building the signal is coming from, nor the type of equipment which is transmitting the interfering signal.

4.7.1 Functions of the Software Module

The "Spectral Scan" software module enables you to run a spectral analysis directly on the access point. There is no need to purchase any additional software or hardware as the integrated functionality can be used to analyze the frequency ranges and bands in question. This gives you a graphical overview of the frequency response characteristics within your WLAN at all times, so that you can detect interference and safeguard against it.

4.7.2 Starting a Spectral Scan

Clicking on the menu option `Extras:Spectral scan` in WEBconfig opens the window shown below:


Spectral Scan
Interfaces
Radio-Bands
Subbands
WLAN-1:
2.4GHz
Band-1+2
Stop
Show
Band-1
Band-2
Band-1+2
The WLAN module "WLAN-2" of this unit is turned off.
Please manually configure the operating mode "Access-Point" or make sure that the device is configured by a WLC.
This page is used to start and stop the spectral scan.
Depending on the current state of the device there will be different buttons and selections available:
Selection "Radio-Bands"
This selection defines which radio bands will be analysed once the spectral scan is started. In case it is running already the selection will be shown greyed-out.
Selection "Subbands"
If 5 GHz is selected as one of the radio bands the selection of subbands will be displayed to allow further specification of the frequency range to be analysed. The selection will be shown greyed-out if the spectral scan is running already.
Button "Start"
The spectral scan is started on the respective WLAN module by pressing this button. For each selected frequency band one additional window will be opened to display the results of the spectral scan. As long as the spectral scan is active, the WLAN module is unavailable for data transfers.
Button "Stop"
Stopping the spectral scan will revert the state of the WLAN module to the previous settings.
Button "Show"
This button will open one window for each selected frequency band to display the results of the spectral scan.

Note: If the WLAN module is disabled (`Setup:Interfaces:WLAN:Operational`), a message is displayed and the spectral scan cannot be started. Configure the access point for "Base station" operation or ensure that a WLAN controller configures the access point.

The following entries, buttons and selection menus are available here:

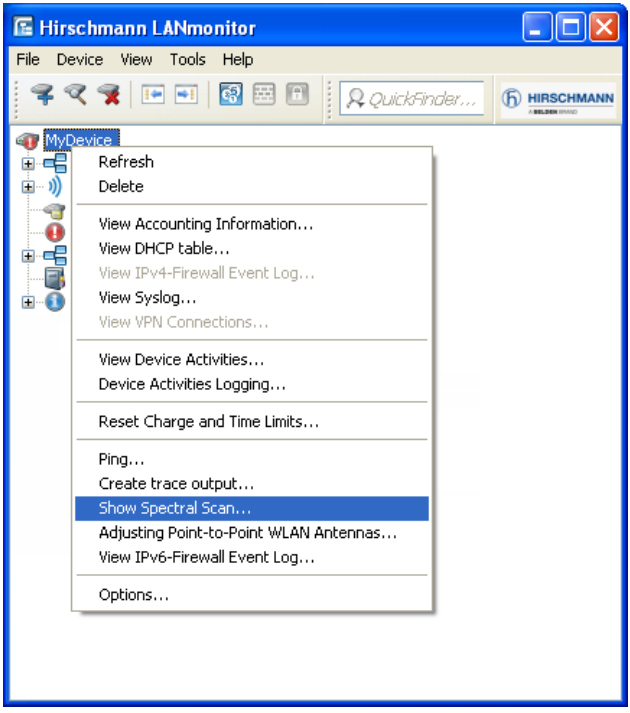
- "Interfaces": Shows the selected WLAN module for analysis.
- "Radio bands": Use this selection menu to set which frequency band(s) you wish to analyze. The relevant field is grayed out once the spectral scan has started on this module.
- "Subbands": This selection menu is only enabled if '5GHz' or '2.4GHz/5Ghz' is selected in "Radio bands". You are then able to specify which sub-bands of the 5GHz band are included in the analysis.

- "Start": Clicking this button starts the spectral scan on the relevant WLAN module. A separate window opens for each of the selected frequency bands.
- "Stop": This buttons ends the analysis. The WLAN module then returns to the previous mode and is available again with its usual functionality.

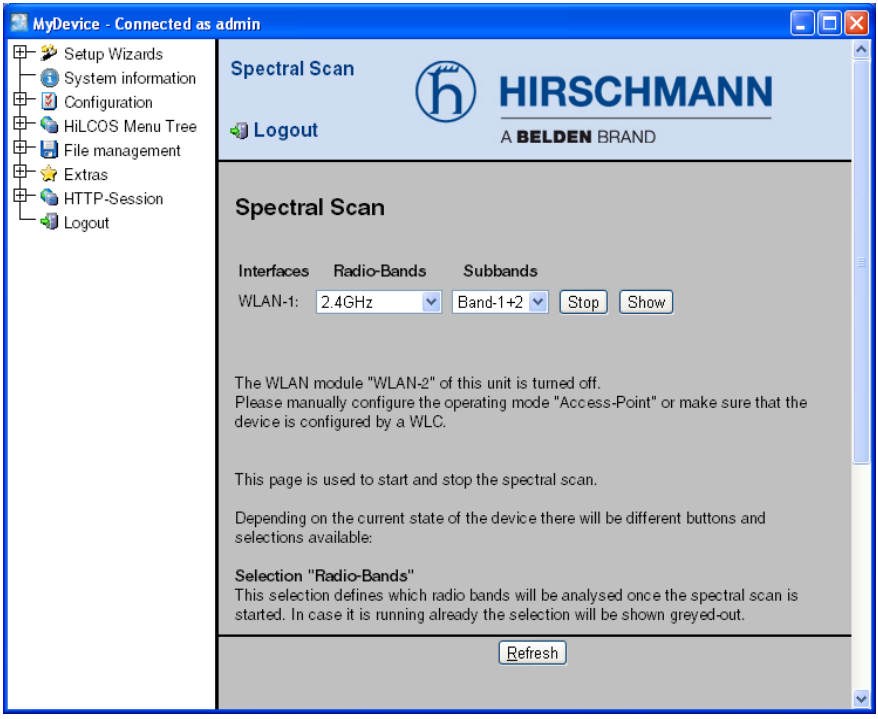
  Note: This button is only shown once the module has been started.
- "Show": Once the spectral scan has started, click this button to open a window for each selected frequency band. Click the button repeatedly to open multiple windows.

Note: During the analysis, the WLAN module being analyzed does not send any data or transmit any SSID.

The spectral scan can also be started from the LANmonitor. To do this, right-click the relevant device in the list and select "Show spectral scan" in the context dialog.



The LANmonitor browser window opens showing you the same entries, buttons and selection menus as those in WEBconfig.


MyDevice - Connected as admin
Setup Wizards
System information
Configuration
HiLCOS Menu Tree
File management
Extras
HTTP-Session
Logout
Spectral Scan
Logout
HIRSCHMANN
A BELDEN BRAND
Spectral Scan
Interfaces
Radio-Bands
Subbands
WLAN-1:
2.4GHz
Band-1+2
Stop
Show
The WLAN module "WLAN-2" of this unit is turned off.
Please manually configure the operating mode "Access-Point" or make sure that the device is configured by a WLC.
This page is used to start and stop the spectral scan.
Depending on the current state of the device there will be different buttons and selections available:
Selection "Radio-Bands"
This selection defines which radio bands will be analysed once the spectral scan is started. In case it is running already the selection will be shown greyed-out.
Refresh

4.7.3 Spectral Scan Analysis Window

Note: The spectral scan is displayed in a browser application. For this to work properly, your browser must support the latest version of WebSockets, and the HTML5 element `<canvas>`. The browser in LANmonitor meets all of these requirements.

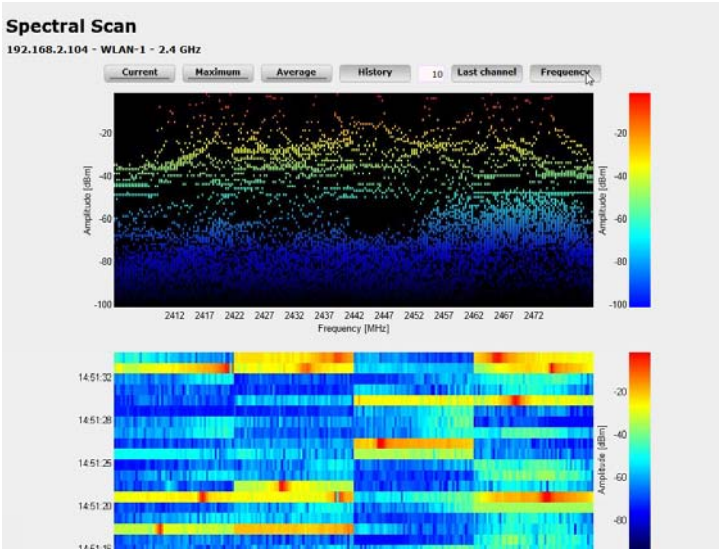
In the separate analysis window of the spectral scan, there are different ways to show the frequencies and frequency ranges together with the potential interference. The following buttons are available at the top of the window:

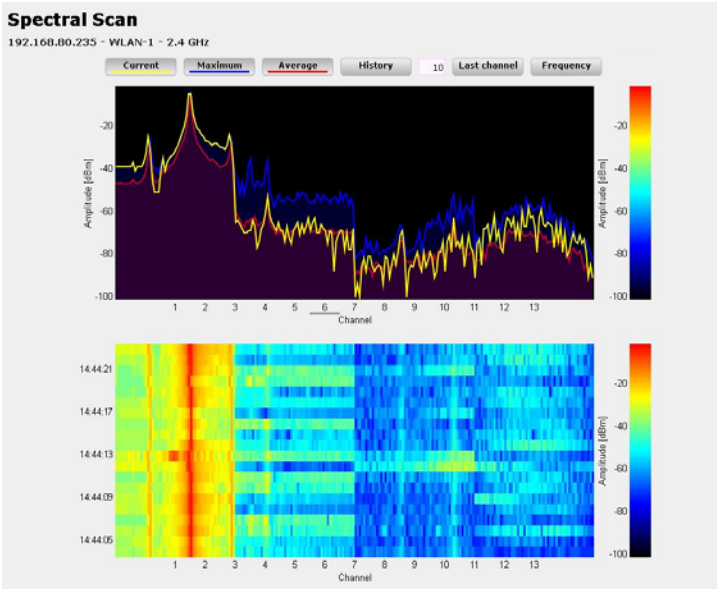
- "Current": Shows or hides the curve of the values being measured.
- "Maximum": Shows or hides the maximum values of the ongoing spectrum scan in relation to the currently set history range.
- "Average": Shows or hides the average values of the ongoing spectral scan in relation to the currently set history range.
- "History": Shows or hides the values last measured.
- "Number of history values": Determines the number of the most recent results to be displayed. You are able to show at least the last 5 and at most the last 50 measuring points for every frequency.
- "Last channel": Shows or hides the channel last used.
- "Frequency": Switches the display on the X-axis between WLAN channel and frequency.

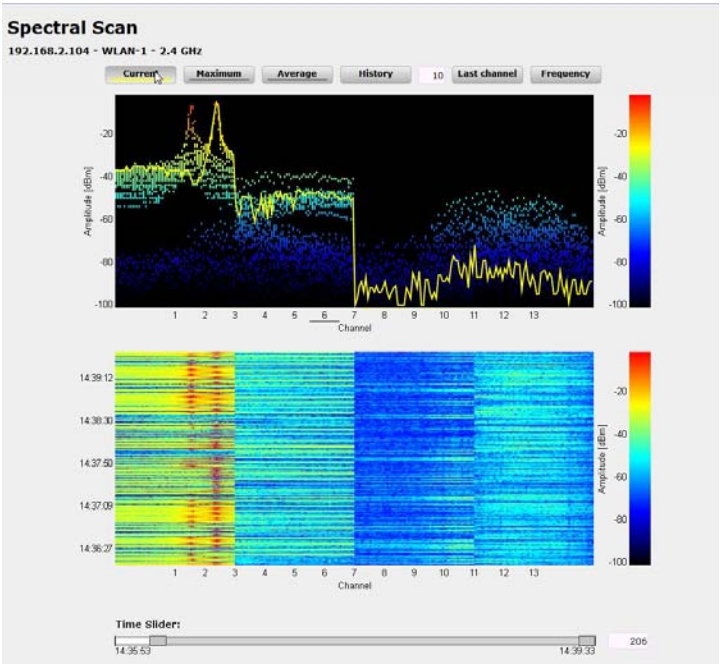
The window contains two graphical views showing the readings in a different manner. The top diagram shows the signal strength in dBm on the Y-axis, and either the WLAN channel or the relevant frequency on the X-axis. The lower diagram contains the analysis progression over time in the form of a waterfall diagram, with the Y-axis showing the time and the X-axis again showing the WLAN channel or the relevant frequency. These view formats depict both continuous and occasional interference on the frequencies, so helping you to take appropriate action to improve the connectivity (e.g. by changing the channel or identifying and eliminating the interference source). For example, certain interference sources such as microwave devices, DECT telephones (working in the 2.4GHz frequency range) and audio-video transmitters exhibit very typical transmit patterns that occur prominently in both diagrams.

On the lower border of the window is a slider denoted "Time slider". This enables you to extend or limit the time period analyzed in the waterfall diagram. Alternatively, you can use the input box to the right of the slider to select how many readings you would like to display in the waterfall diagram. The web application can display up to 300 readings in the waterfall diagram using the time slider. The readings from a maximum of 24 hours can be cached.

Below are some example analysis results showing graphically other settings in a different way:




Spectral Scan
192.168.80.235 - WLAN-1 - 2.4 GHz
Current
Maximum
Average
History
10
Last channel
Frequency
Amplitude [dBm]
Channel
14:44:21
14:44:17
14:44:13
14:44:09
14:44:05


Spectral Scan
192.168.2.104 - WLAN-1 - 2.4 GHz
Current
Maximum
Average
History
10
Last channel
Frequency
Amplitude [dBm]
Channel
14:38:12
14:38:30
14:37:50
14:37:09
14:36:27
Time Slider:
14:35:53
14:39:33
206

4.8 Extended WLC Functions

4.8.1 Automatic Radio-Field Optimization with Hirschmann WLAN-Controllers

With the selection of the channel from the channel list, you define the part of the frequency band that an Access Point uses for its logical WLANs. All WLAN Clients that connect to an Access Point must use the same channel on the same frequency band. In the 2.4-GHz band, channels 1 to 13 are available (depending on the country), and in the 5-GHz band, channels 36 to 64 are available. At a given point in time, only one Access Point transmits its data on one channel. For a WLAN to reach maximum bandwidth within the radio range of another Access Point, use a separate channel for each Access Point. Otherwise the WLANs share the channel's bandwidth.

Note: With a completely open channel list, the Access Points might automatically select channels that overlap in some areas, resulting in a loss in signal quality. Similarly, the Access Points might select channels which the WLAN Clients cannot use due to the country settings. To direct Access Points towards certain channels, activate e.g. the non-overlapping channels 1, 6, 11 in the channel list.

In larger installations, selecting a suitable channel for every Access Point can be difficult. Automatic radio-field optimization is a method offered by Hirschmann WLAN-Controllers where the optimum channels for the Access Points in the 2.4-GHz band are automatically set.
WEBconfig: Setup > WLAN-Management > Start-automatic-radio-field-optimization

Note: Optionally start the optimization for an individual Access Point by entering the MAC address as parameter for the action.

LANmonitor: Right-click an active Access Point and select "Start automatic RF optimization" from the context menu.

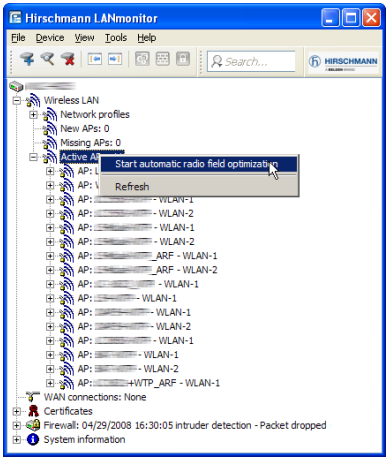


Figure 34: Setting automatic radio-field optimization

Optimization is then carried out in the following steps:

- ☐ The WLAN-Controller deletes the AP channel list of all Access Points in the 2.4-GHz range. As the channel list for the Access Points is then empty, the WLAN-Controller transmits the channel list of its profile by means of a configuration update.
- ☐ The WLAN-Controller switches off all radio modules operating in the 2.4-GHz range.
- ☐ The WLAN-Controller switches on the Access Point one after the other. During this process, the WLAN-Controller observes the sequence in which the Access Points registered.

- Automatic calibration: After the Access Point is switched on, it selects the optimum channel from the channel list. To determine the optimum channel, the Access Point carries out an interference measurement that considers the signal strengths and channels of all Access Points from the profile channel list in the WLAN-Controller. When the profile channel list is empty, the Access Point selects from all free channels.
- The Access Point transmits the selected channel to the WLAN-Controller, which saves it in the AP channel list. Therefore the Access Point receives the same channel the next time a connection is established. The AP channel list thus has a higher weighting than the profile channel list.

Note: If an Access Point is equipped with multiple WLAN modules, the Access Point will repeat this process for every WLAN module.

4.8.2 Central Firmware and Script Management

With Hirschmann WLAN-Controller, you can configure multiple Access Points consistently and conveniently from one location. With central firmware and script management, firmware and script uploads can be started automatically on all managed WLAN devices.
For this purpose, store the firmware and script files on a web server (firmware as *.UPX files, scripts as *.LCS files). Once daily or when prompted by a user, the WLAN-Controller compares the available files with the versions in the devices. Alternatively, this procedure can be handled by a cron job . e.g. overnight. The WLAN-Controller downloads files from the web server and uploads them into the corresponding Access Points if one of the following conditions applies:

- The server contains a newer version of the file.
- The Access Point runs with another version than the desired one.

With the configuration of firmware and script management, you control the distribution of the files. It is thus possible to limit the use of certain firmware versions e.g. to specific device types or MAC addresses.

The WLAN-Controller starts the update under 2 possible conditions:

- ☐ When a connection is established, the Access Point subsequently restarts automatically.
- ☐ When the Access Point is already connected, the device does not restart automatically. In this case start the Access Point manually via the menu action "/Setup/WLAN-Management/Central-Firmware-Management/Reboot-updated-APs" or via a timed cron job.

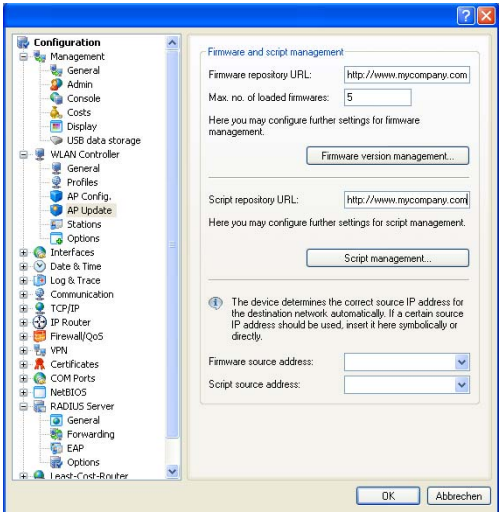


Figure 35: Configuring the firmware and script management

You will find the configuration parameters on the following paths:
LANconfig: WAN Controller > AP Update
WEBconfig: Setup > WLAN Management > Central Firmware Management

General Settings for the Firmware Management

☐ Firmware URL:
Path to the firmware-files directory.
- Possible values: URL in the form `Server/Directory` or `http://Server/Directory`
- Default: blank

☐ Simultaneously loaded FW
The number of firmware versions loaded simultaneously into the main memory of the WLAN-Controller.
- Possible values: 1 to 10
- Default: 5

Note: The WLAN-Controller downloads the firmware versions stored here just once from the server and then uses them for all suitable update processes.

☐ Firmware Sender IP Address
This is where you can configure an optional sender address that the device can use instead of the one automatically selected for the destination address.
Possible values:
- Name of a defined IP network.
- 'INT' for the IP address in the first network with the setting 'Intranet'.
- 'DMZ' for the IP address in the first network with the setting 'DMZ'.
- Name of a loopback address.
- Any other IP address.
- Blank (default):

Note: If the lists of IP networks or loopback addresses contains an entry named 'INT' or 'DMZ', the associated IP address of the IP network or the loopback address named 'INT' or 'DMZ' is used.

Firmware Management Table

Table with device type, MAC address and firmware version for the precise control of the firmware files in use.

☐ Device types
Here select the type of device that the firmware version specified here is to be used for.
- Possible values: Selection from the list of available device types.
- Default: All

- ☐ MAC address
  Here select the device (identified by its MAC address) that the firmware version specified in this entry is to be used for.
  - ▶ Possible values: Valid MAC address.
  - ▶ Default: Blank
- ☐ Version
  Firmware version that is to be used for the devices or device types specified in this entry.
  - ▶ Possible values: Firmware version in the form X.XX
  - ▶ Default: Blank

General Settings for the Script Management

- ☐ Script URL
  Path to the script-files directory.
  - ▶ Possible values: URL in the form `Server/Directory` or `http://Server/Directory`
  - ▶ Default: Blank
- ☐ Script sender IP address
  Here you can configure an optional sender address that the device can use instead of the one automatically selected for the destination address.
  Possible values:
  - ▶ Name of a defined IP network.
  - ▶ 'INT' for the IP address in the first network with the setting 'Intranet'
  - ▶ 'DMZ' for the IP address in the first network with the setting 'DMZ'
  - ▶ Name of a loopback address
  - ▶ Any other IP address.
    Default:
  - ▶ Blank

Note: If the lists of IP networks or loopback addresses contains an entry named 'INT' or 'DMZ', the associated IP address of the IP network or the loopback address named 'INT' or 'DMZ' is used.

Script Management Table

The table contains the script file names and the assigned WLAN profiles.

An Access Point in the operating mode "managed" is configured via WLAN profiles. With a script, you can also set those detailed parameters in managed devices that exceed the pre-defined parameters in a WLAN profile. The assignment is also implemented via the WLAN profiles to ensure that Access Points with the same WLC configuration also use the same script.
As only one script file can be defined for each WLAN profile, versioning is not possible. When a script is assigned to an Access Point, however, the WLAN-Controller saves an MD5 check sum of the script file. This checksum allows the WLAN-Controller to determine whether the script file has to be transmitted again if a new or altered script file has the same file name.

- ☐ Script file name
  Name of the script file to be used.
  - ▶ Possible values: File name in the form *.lcs
  - ▶ Default: blank
- ☐ WLAN profile
  Select here for which WLAN profile the script file specified in this entry is to be used.
  - ▶ Possible values: Selection from the list of defined WLAN profiles.
  - ▶ Default: Blank

Internal Script Memory (Script Management without HTTP Server)

Unlike firmware files, scripts often have small data volumes. The WLAN-Controller's internal script memory can hold 3 scripts of a maximum size of 64 kB each. If this storage capacity is sufficient for your scripts, you do not need to set up an HTTP server for this purpose.
Simply load the script files using WEBconfig to one of the 3 storage locations. After the upload, update the list of available scripts using the action Setup/WLAN Management/Central Firmware Management/ Update Firmware and Script Information.
From the script management table, reference these internal scripts using the relevant names (WLC_Script_1.lcs, WLC_Script_2.lcs or WLC_Script_3.lcs).

Note: Please observe the case sensitivity when entering script names.

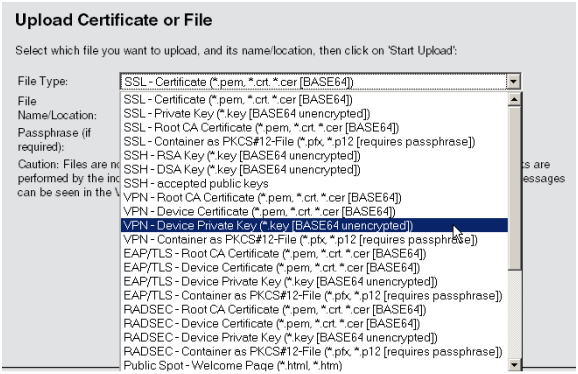


Figure 36: Uploading script files via WEBconfig

4.8.3 Checking WLAN Clients with RADIUS (MAC Filter)

When using RADIUS to authenticate the WLAN Clients, you can use the internal user table of the Hirschmann WLAN-Controller as an alternative to an external RADIUS server. The user table only grants specific WLAN Clients access to the WLAN, based on their MAC address.
Enter the approved MAC addresses in LANconfig into the RADIUS database in the configuration section 'RADIUS servers' on the 'General' tab. Enter the MAC address as 'Name / MAC address' and also as 'Password' and allow all protocols for authentication (no restrictions).

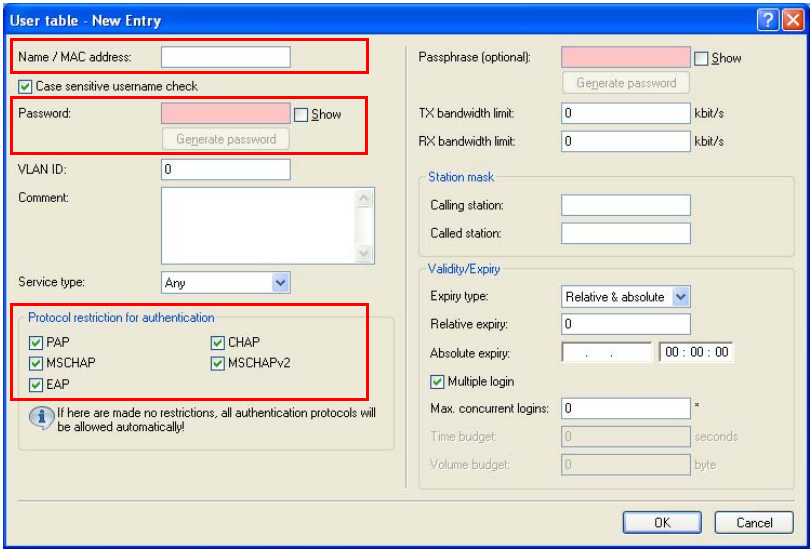


Figure 37: Creating a new user account

Alternatively, enter the approved MAC addresses in WEBconfig under HiLCOS menu tree > Setup > RADIUS > Server > Users.

Note: As 'Name / MAC address' and as 'Password', enter the MAC address in the form 'AABBCC-DDEEFF'.

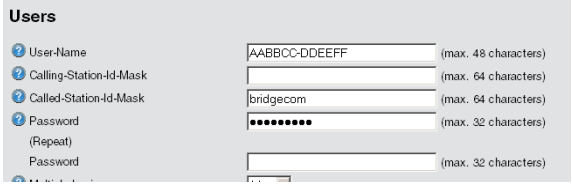


Figure 38: Creating a new user account using WEBconfig

4.8.4 Separate RADIUS Server for Each SSID

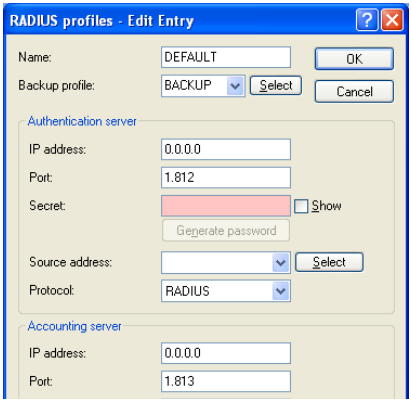
If you operate RADIUS for the central administration of accounts and credentials in your wireless network, then the access point forwards requests for the authorization and accounting to the RADIUS server by default. If you are using a WLAN controller for access point management, then the controller can forward RADIUS requests from all of these access points to the RADIUS server.

In some cases, the operator of access points or WLAN controllers may wish to use a different RADIUS server for each logical wireless network (SSID). This may be the case, for example, when multiple customers share the same technical WLAN infrastructure but use their own authentication systems (e.g. with Wireless as a Service – WaaS).

In these cases, you have the option to choose a separate RADIUS profile for each logical WLAN (i.e. each SSID). The RADIUS profile contains all of the necessary information to use the appropriate RADIUS server, including the optional backup solution.

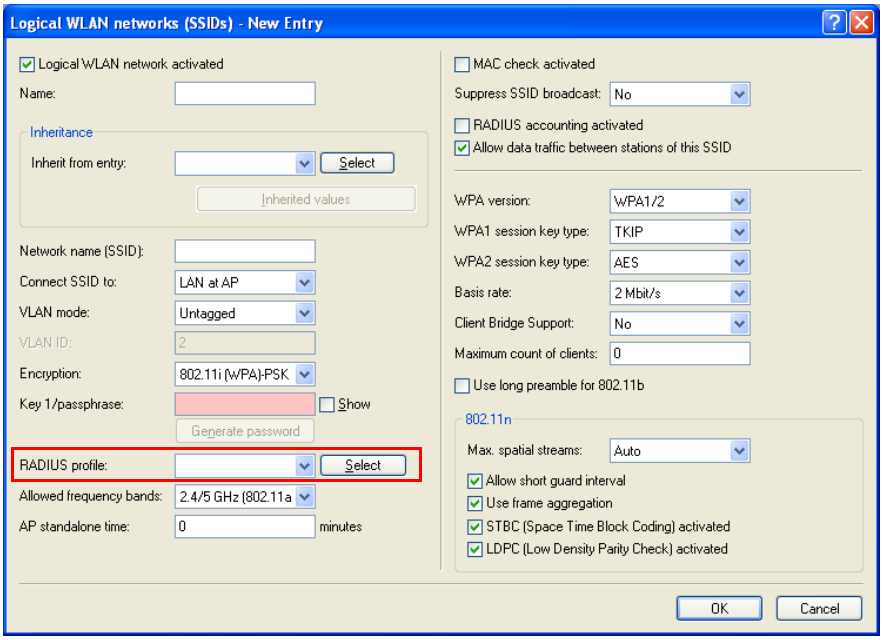
Setting up the RADIUS Profiles

In LANconfig, the settings for the RADIUS profiles in the WLAN controller are to be found under `WLAN Controller:Profiles:RADIUS profiles`.



Selecting a RADIUS Profile for a Logical WLAN

In LANconfig, selecting the RADIUS profile for a logical WLAN in the WLAN Controller is done with the menu item `WLAN Controller:Profiles:Logical WLAN networks`.



4.8.5 Dynamic VLAN Assignment

In larger WLAN structures, it is often advisable to assign a specific network to the individual WLAN Clients. As long as the WLAN Clients are always within the coverage area of the same Access Point, you can realize this assignment via the SSID in connection with a particular IP network. If the WLAN Clients often change their position, however, and log into different Access Points, they will be in a different IP network, depending on the configuration.
Use dynamically assigned VLANs to direct the WLAN Clients from different WLAN networks to a specific IP network. Unlike it is the case with statically configured VLAN IDs for a specific SSID, the RADIUS server transmits the VLAN ID directly to the WLAN Client.
Example:

- ☐ The WLAN Clients of the employees use an Access Point to log into the WPA-secured wireless network with the SSID 'INTERNAL'. During registration, the RADIUS requests of the WLAN Clients are directed to the Access Point. If the corresponding WLAN interface is in the operating mode 'managed', the RADIUS requests are automatically forwarded to the WLAN-Controller. This in turn forwards the requests to the configured RADIUS server. The RADIUS server checks the access rights of the WLAN Clients. It also transmits, e.g. based on the MAC address, a certain VLAN ID for the respective department. The WLAN Client from Marketing, for example, will receive the VLAN ID '10', and the WLAN Client from Development the VLAN ID '20'. If no VLAN ID is defined for the user, the device transmits the primary VLAN ID of the SSID.
- ☐ The WLAN Clients of the guests use the same Access Point to log into the unsecured wireless network with the SSID 'PUBLIC'. This SSID is statically linked to the VLAN ID '99' and thus directs the guests into a specific network. You can optionally use the static and dynamic VLAN assignment in parallel.

Note: The assignment of the VLAN ID by the RADIUS server can alternatively be controlled by other criteria, such as the combination of user name and password. Thus the RADIUS server will, for example, assign a specific VLAN ID to the unknown MAC addresses of a company's visitors. This VLAN for guest access will, e.g., grant access to the Internet only, but no access to any other network resources.

Note: As an alternative to an external RADIUS server, the internal RADIUS server or the station table in the Hirschmann WLAN-Controller can transmit a VLAN ID to the WLAN Clients.

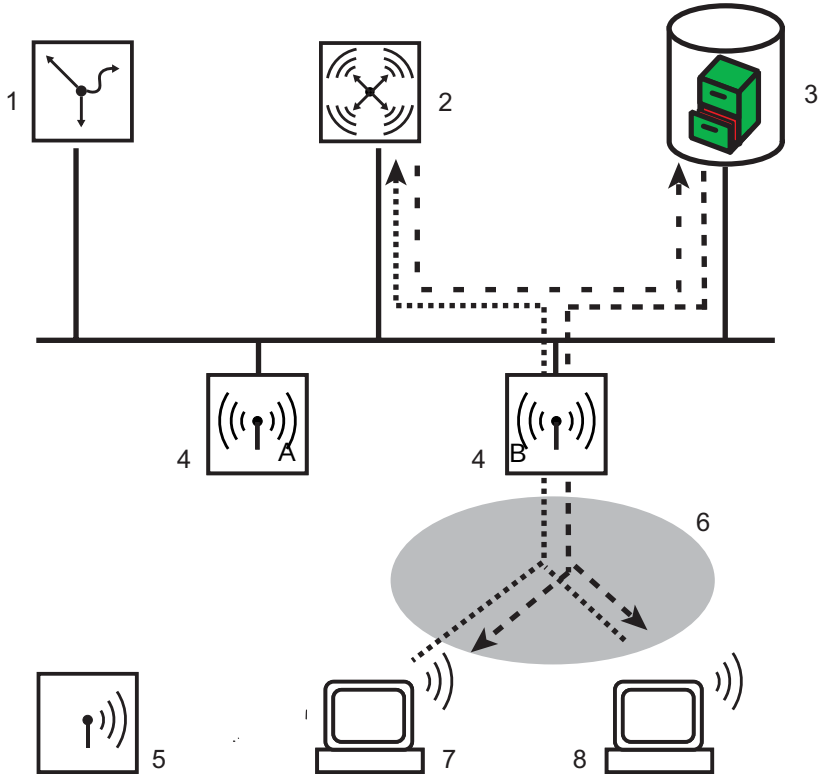


Figure 39: Dynamic VLAN assignment

1: Hirschmann VPN router
2: WLAN Controller
3: RADIUS server
4: Access Point
5: WLAN Clients
6: SSID 'INTERNAL'
7: VLAN-ID '10'
8: VLAN-ID '20'

☐ Activate VLAN tagging for the WLAN-Controller. This is done in the physical parameters of the profile by entering a value greater than '0' as management VLAN ID.
☐ For authentication via 802.1x, go to the encryption settings for the profile's

logical WLAN network and choose a setting that triggers an authentication request.

☐ To check the MAC addresses, activate the MAC check for the profile's logical WLAN network.

Note: For the management of WLAN modules with a WLAN-Controller, a RADIUS server is required both for the authentication via 802.1x and for the MAC-address checks. The WLAN-Controller automatically defines itself as RADIUS server in the Access Points it is managing. The Access Points send all incoming RADIUS requests to the WLAN-Controller, which either processes the requests itself or forwards it to an external RADIUS server.

Note: Further information about RADIUS is available in the documentation for your RADIUS server.

Note: Further information about RADIUS is available in the documentation for your RADIUS server.

4.8.6 Load Balancing between the WLAN-Controllers

If multiple WLAN-Controllers are available in a network, the WLAN-Controllers automatically distribute the Access Points evenly among each other.

At the beginning of the communication, the Access Point sends a "Discovery Request Message" to identify the available WLAN-Controllers.

- ☐ If the Access Point gets responses from primary and secondary WLAN-Controllers, it prefers primary controllers.
- ☐ From the available WLAN-Controllers, the Access Point selects the one with the lowest load. This is the WLAN-Controller with the lowest ratio of managed Access Points to maximum possible Access Points.
- ☐ In case of two or more equally utilized WLAN-Controllers, the Access Point selects the WLAN-Controller with the fastest response time.

So by activating several WLAN-Controllers via automatic assignment of configurations, for example, all WLAN-Controllers are equally filled with configurations for a proportion of the Access Points.

4.8.7 WLAN Layer-3 Tunneling

The CAPWAP standard for centralized WLAN management offers 2 different transmission channels:

- ☐ The obligatory control channel transfers management data between the managed Access Point and the WLAN Controller.
- ☐ The optional data channel transfers the payload data from the respective WLAN networks (SSID) between the managed Access Point and the WLAN Controller.

The optional use of the data channel between the managed Access Point and the WLAN Controller determines the path of the payload data:

☐ If you deactivate the data channel, the Access Point forwards the payload data directly into the LAN. In this case you control the assignment of WLAN Clients to specific LAN segments e.g. via the assignment of VLAN IDs. The advantage of this application is, above all, the low load placed on the controller and the entire network. The Access Point transmits only the management data via the CAPWAP tunnel, the payload data is transmitted over the shortest path.

☐ If you activate the data channel, the Access Point also transmits the payload data to the central WLAN Controller. This approach has the following advantages:

- The Access Points optionally propagate networks that are exclusively available on the Controller, e.g. a central Internet access for a public spot.
- The WLANs (SSIDs) offered by the Access Points are also available separately, without the use of VLAN. Refraining from the use of VLAN reduces the effort for the configuration of other network components, such as switches, etc.
- The WLAN Clients logged into different IP networks at the Access Points are roaming to another Access Point with an uninterrupted IP connection. The controller subsequently manages the connection instead of the Access Point (layer-3 roaming).

With the use of the data channel, additional logical networks, referred to as overlay networks (displayed as dotted lines in the following illustration), are created on the basis of the existing physical network structure.

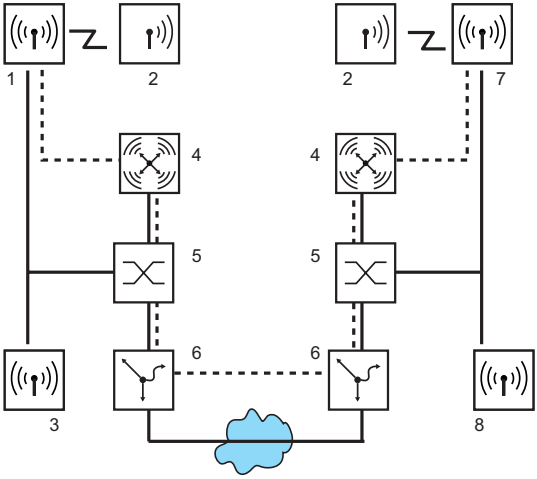


Figure 40: Overlay networks across several IP networks

1: IP network Plant 1 Production
2: WLAN Client
3: IP network Plant 1 Warehouse
4: WLAN Controller
5: Layer-3 switch
6: Gateway
7: IP network Plant 2 Production
8: IP network Plant 2 Warehouse

Via the data channel, you can even establish logical overlay networks across various WLAN Controllers.
Several WLCs that are supporting the same overlay network require separate broadcast domains. The multiple reception of the broadcast news otherwise leads to loops within a broadcast domain. As routers drop the broadcast news, two controllers in separate networks manage the same overlay networks, if necessary.
The Access Points use virtual WLC interfaces (WLC tunnels) to manage the data channels of the respective SSIDs between the Access Point and the WLAN Controller. Depending on the model, every WLAN Controller offers 16 to 32 WLC tunnels that are available for the configuration of the logical WLANs.

Note: The devices contain the virtual WLC interfaces in all dialogs for the selection of logical interfaces (LAN, WLAN, P2P). You can find this selection, e.g. in the port tables of the LAN and VLAN settings or in the definition of IP networks.

4.9 Application Examples

In the following sections you will find specific scenarios with step-by-step instructions for a range of standard scenarios using WLAN controllers.

4.9.1 "Overlay Network": Separating Networks for Access Points without VLAN

The separation of networks within a common, shared physical infrastructure is mostly based on the use of VLANs. This process requires that the switches used are VLAN-capable, however, and that all switches have the corresponding VLAN configurations. In this example, the administrator distributes the VLAN configuration across the entire network.
With a WLAN Controller, you can also separate the networks with a minimum use of VLANs. Through a CAPWAP data tunnel, the Access Points transmit the payload data of the connected WLAN Clients directly to the Controller, which assigns the data to the corresponding VLANs. Here the VLAN configuration is limited to the Controller and a single central switch. All other switches work without VLAN configuration in this example.

Note: This configuration helps you to reduce the VLAN to the core of the network structure (displayed in blue in the illustration.) In addition, only 3 of the switch ports used require a VLAN configuration.

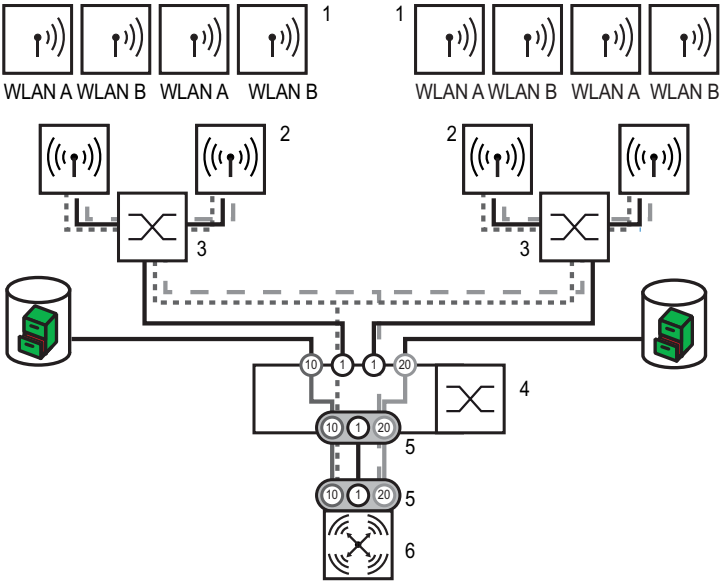


Figure 41: Application example overlay network

1: WLAN Client
2: Access Point
3: Unmanaged switch
4: VLAN switch
5: VLAN trunk, several VLAN IDs
6: WLAN Controller
Black line: No VLAN, in VLAN switches on VLAN-ID 1 displayed as 'native VLAN'
Dark gray dotted line: WCL tunnel group A
Dark gray line: VLAN group A
Light gray dashed line: WCL tunnel group B
Light gray line: VLAN group B
The numbers in circles indicate the VLAN ID

The illustration shows an application example with the following components:

- The network consists of 2 segments, each with its own switch (optionally without VLAN function).
- There are several Access Points in every segment, connected to the respective switch.
- Every Access Point offers 2 SSIDs for the WLAN Clients of different user groups, displayed in green and orange in the illustration.
- Every user group has access to their own server, protected from the access of other user groups. The servers can only be reached via the corresponding VLANs through the access ports configured on the switch.
- A WLAN Controller manages all Access Points in the network.
- A central, VLAN-capable switch connects the switches of the segments, the group-related servers and the WLAN Controller.

The aim of the configuration: A WLAN Client that logs into a specific SSID can access "its" server in every segment.

Note: The following description applies to a WLAN Controller with functional basic configuration. For instructions regarding the configuration of the VLAN switch, please refer to the relevant documentation.

Configuration of the WLAN Settings

- For each SSID, create an entry in the list of logical networks with a suitable name and the corresponding SSID. Connect this SSID to a WLC tunnel, the first SSID e.g. to 'WLC-TUNNEL-1' and the second one to 'WLC-TUNNEL-2'. Set the VLAN operating mode to 'tagged' in both cases, with the VLAN ID '10' for the first logical network and the VLAN ID '20' for the second logical network. In LANconfig, you can find these settings under Configuration/WLAN Controller/Profiles/Logical WLAN networks (SSIDs).

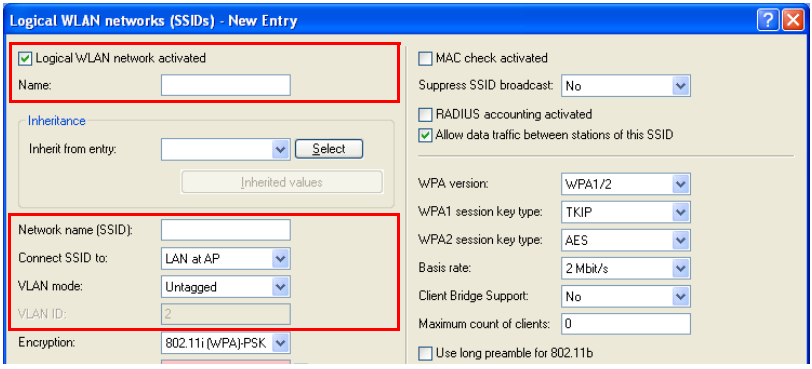


Figure 42: Logical WLAN networks for overlay networks

- Create an entry in the list of physical WLAN parameters. Select the suitable settings for your Access Points, e.g. for the country 'Europe', with channels 1, 6 and 11 in 802.11g/b/n and 802.11a/n mixed mode. For this profile of physical WLAN parameters, activate the option to switch on the VLAN module on the Access Points. Use 'untagged' as operating mode for the management VLAN in the Access Points. In LANconfig, you can find these settings under Configuration/WLAN Controller/Profiles/ Physical WLAN parameters.

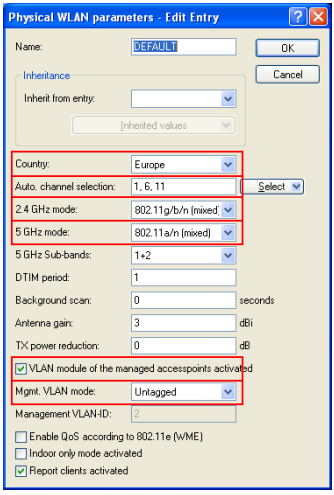


Figure 43: Physical WLAN parameters for overlay networks

- Create a WLAN profile with an appropriate name and select the previously created logical WLAN networks and the physical WLAN parameters for this WLAN profile. In LANconfig, you can find these settings under Configuration/WLAN Controller/Profiles/Physical WLAN profiles.

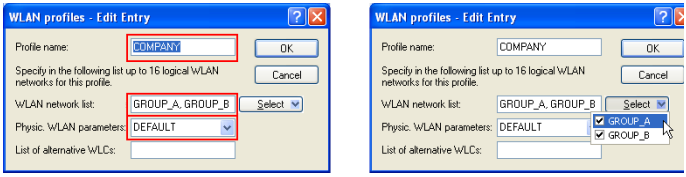


Figure 44: WLAN profiles for overlay networks

- For every managed Access Point, create an entry in the access-point table with an appropriate name and the corresponding MAC address. Select the previously created WLAN profile for this Access Point. In LANconfig, you can find these settings under Configuration/WLAN Controller/AP config/Access-point table.

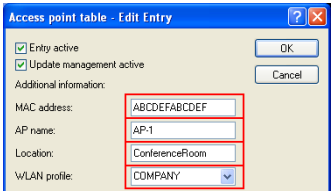


Figure 45: Access-point table for overlay networks

Configuration of the Interfaces on the WLC

- For every physical Ethernet port, select a separate logical LAN interface, e.g. 'LAN-1'. Make sure that further Ethernet ports use other LAN interfaces exclusively. In LANconfig, you can find these settings under Configuration/Interfaces/LAN/Ethernet ports.

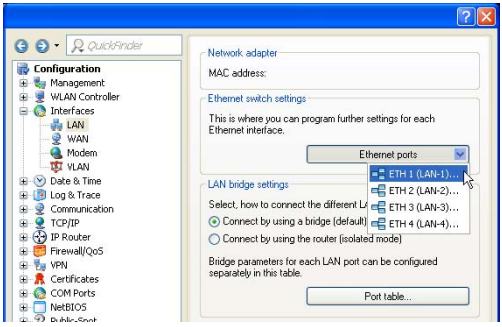


Figure 46: Ethernet settings for overlay networks

- Select the logical LAN interface 'LAN-1' and the WLC tunnels 'WLC-tunnel-1' and 'WLC-tunnel-2' for the Bridge group 'BRG-1'. Make sure that the other LAN interfaces use other bridge groups exclusively. In LANconfig, you can find these settings under Configuration/Interfaces/LAN/Port table.

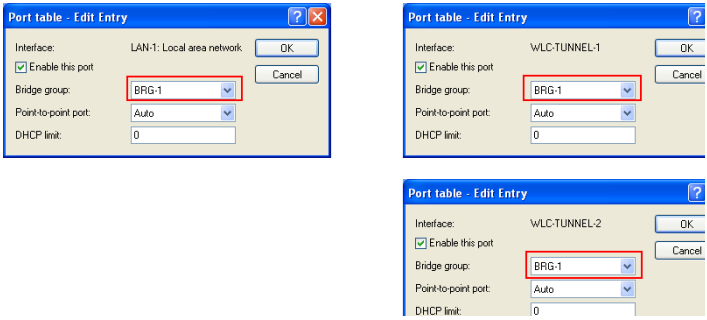


Figure 47: Port settings for overlay networks

Note: By default, the LAN interfaces and the WLC tunnel do not belong to any bridge group. If you assign the LAN interface 'LAN-1' and the two WLC tunnels 'WLC-tunnel-1' and 'WLC-tunnel-2' to the bridge group 'BRG-1', the device transmits all data packets between LAN-1 and the WLC tunnels via the bridge.

- The WLAN Controller can optionally function as DHCP server for the Access Points. To do this, enable the DHCP server for the 'INTRANET'. In LANconfig, you can find these settings under Configuration/IPv4/DHCPv4/DHCP networks.

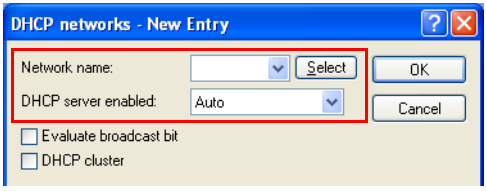


Figure 48: DHCP network for overlay networks

4.9.2 "Layer-3 Roaming"

The forwarding of payload data from the WLANs over WLC tunnels to the Controller permits roaming even beyond the boundaries of broadcast domains. In this application example, a layer-3 switch between the floors prevents the forwarding of broadcasts and thus separates the broadcast domains.
In this example, two user groups, A and B, each have access to their own WLAN (SSID). The Access Points on various floors of the building offer the two SSIDs 'GROUP_A' and 'GROUP_B'.

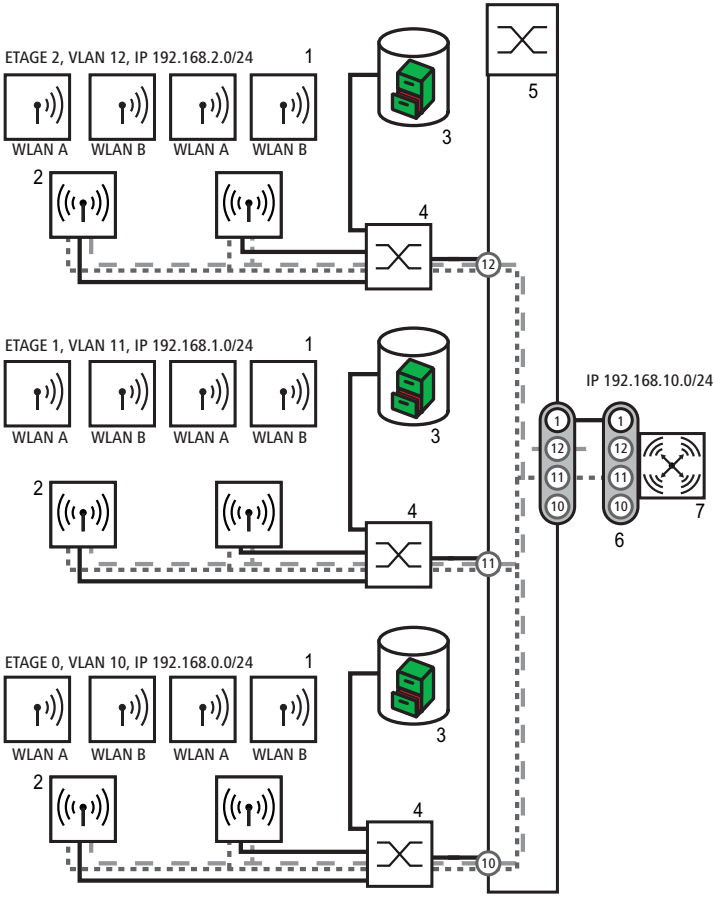


Figure 49: Application example for layer-3 roaming

1: WLAN Client
2: Access Point
3: DHCP Server
4: Unmanaged switch
5: VLAN switch
6: VLAN trunk, several VLAN IDs
7: WLAN Controller
Black line: No VLAN, in VLAN switches on VLAN-ID 1 displayed as 'native VLAN'

Dark gray dotted line: WCL tunnel group A
Dark gray line: VLAN group A
Light gray dashed line: WCL tunnel group B
Light gray line: VLAN group B
The numbers in circles indicate the VLAN ID

The illustration shows an application example with the following components:

- The network consists of three segments on separate floors of the building.
- A central layer-3 switch connects the segments and splits the network into three broadcast domains.
- Each segment uses its own IP address range and its own VLAN.
- In every segment, there is a local DHCP server, transmitting the following information to the Access Points:
  - IP address of the gateway
  - IP address of the DNS server
  - Domain suffix

  Note: The provision of this information enables the Access Points to contact the WLC controller in a different broadcast domain.

The aim of the configuration: A WLAN Client logging into a specific SSID shall have uninterrupted access to "its" WLAN when changing floors - regardless of the Access Point used and regardless of the segment in which it is currently located. As the segments in this example use different IP address ranges, this can only be achieved by managing the Access Points on layer 3 directly via the central WLAN Controller across the VLAN boundaries.

Note: The configuration corresponds to that of the example.

4.9.3 WLAN Controller with Public Spot

This scenario is based on the first scenario (overlay network) and adds specific settings for a user authentication. The forwarding of payload data from the WLANs over WLC tunnels to the controller permits a particularly simple configuration of public spots. Guests, for example, can use these in parallel to an internally used WLAN.
In this example, the employees of a company can access their own WLAN (SSID), guests can also access the Internet via a public spot. The Access Points in all areas of the building offer the two SSIDs 'COMPANY' and 'GUESTS'.

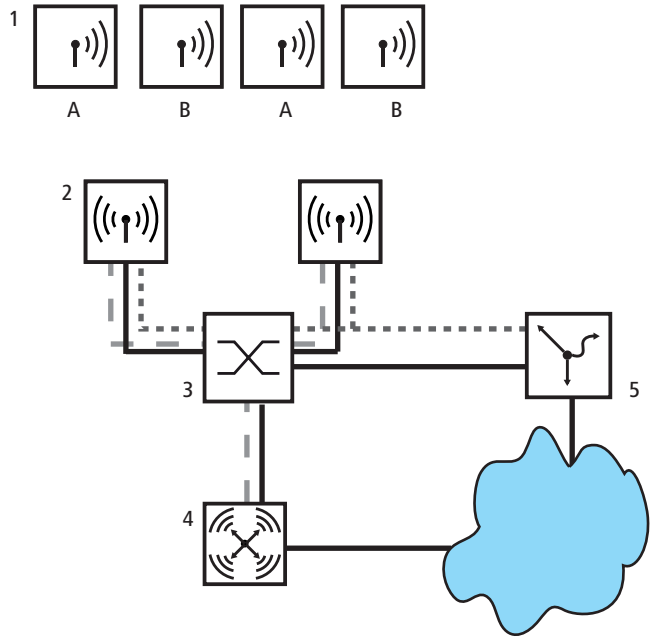


Figure 50: Application example WLAN Controller with public spot
1: WLAN Client
2: Access Point
3: Switch
4: WLAN Controller

5: Gateway
A: Guest access
B: Internal WLAN
Dark gray dotted line: WLC tunnel internal WLAN
Light gray dashed line: WLC tunnel public spot

The aim of the configuration: A WLAN Client logging into the internal SSID shall have access to all internal resources and to the Internet via the central gateway. The Access Points decouple the internal Clients' payload data locally and forward them directly into the LAN. The guests' WLAN Clients log into the public spot. The Access Points forward the guest clients' payload data over a WLC tunnel directly to the WLAN Controller, which provides Internet access via a separate WAN interface.

- Create one entry each for the internal WLAN and the guest WLAN in the list of logical networks, including an appropriate name and the corresponding SSID. Connect the SSID for internal use to the 'LAN on AP', the SSID for the guests to, e.g., 'WLC-TUNNEL-1'. In the SSID for the guest network, deactivate the encryption so that the guests' WLAN Clients can log into the public spot. Inhibit data traffic between the stations for this SSID (interstation traffic). In LANconfig, you can find this setting under Configuration/WLAN Controller/Profiles/Logical WLAN networks (SSIDs).

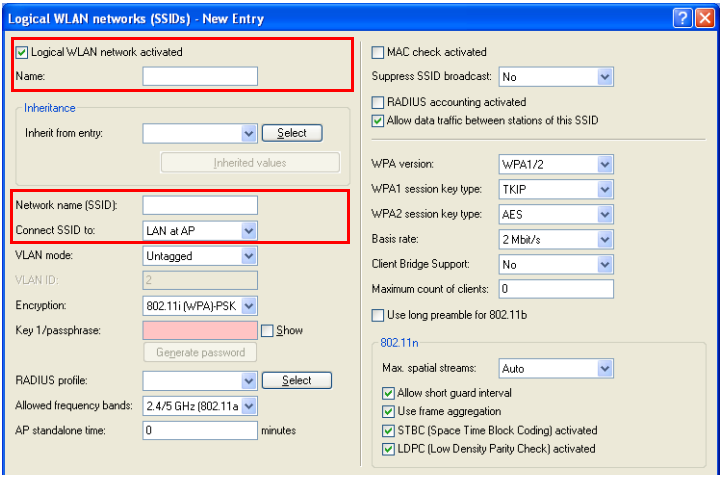


Figure 51: Logical WLAN networks for internal use

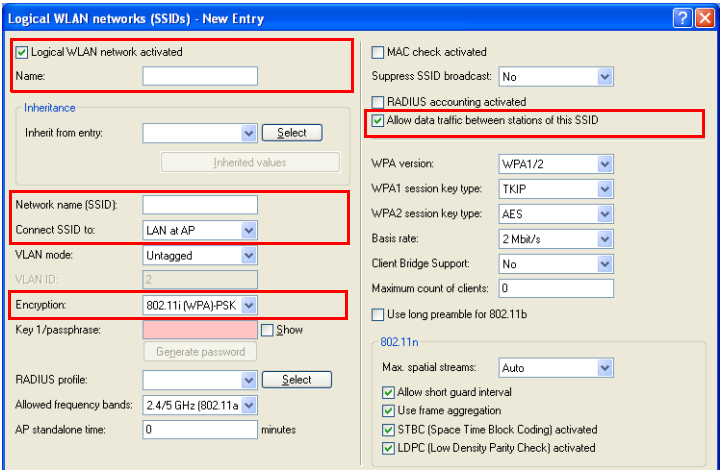


Figure 52: Logical WLAN networks for guest access

- Create an entry in the list of physical WLAN parameters with the suitable settings for your Access Points, e.g. for the country 'Europe', with the channels 1, 6 and 11 in 802.11g/b/n and 802.11a/n mixed mode. In LANconfig, you can find this setting under Configuration/WLAN Controller/Profiles/Physical WLAN parameters.

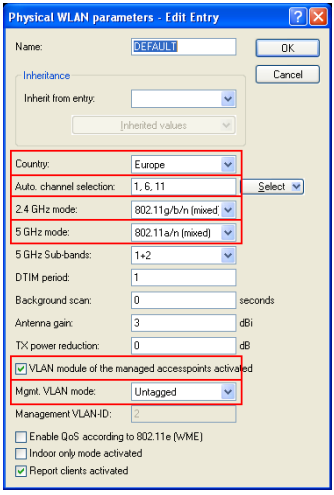


Figure 53: Physical WLAN parameters for public-spot APs

- Create a WLAN profile with an appropriate name and assign the previously created logical WLAN networks and the physical WLAN parameters to this WLAN profile. In LANconfig, you can find this setting under Configuration/WLAN Controller/Profiles/Physical WLAN profiles.

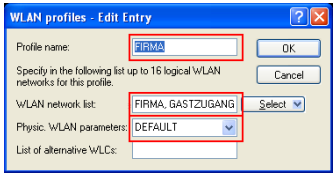


Figure 54: WLAN profiles for public-spot APs

- For every managed Access Point, create an entry in the access-point table with an appropriate name and the corresponding MAC address. Assign the previously created WLAN profile to this Access Point. In LANconfig, you can find this setting under Configuration/WLAN Controller/AP config/Access-point table.

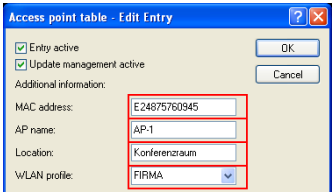


Figure 55: Access-point table for public-spot APs

- Assign a separate logical LAN interface to each physical Ethernet port, e.g. 'LAN-1'. Set the fourth Ethernet port to the logical LAN interface 'DSL-1'. The WLAN Controller uses this LAN interface later for the Internet access of the guest network. In LANconfig, you can find this setting under Configuration/Interfaces/LAN/Ethernet ports.

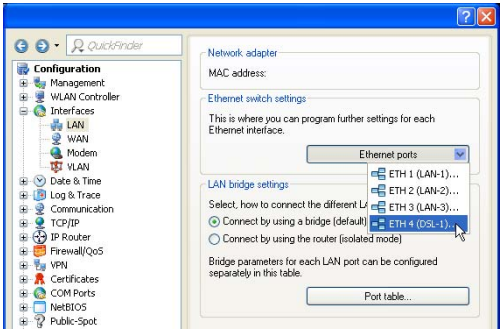


Figure 56: Ethernet settings for public-spot APs

- Check that the logical LAN interface 'WLC-tunnel-1' is not assigned to any bridge group. You thus ensure that the other LAN interfaces do not transmit any data to the public-spot network. In LANconfig, you can find this setting under Configuration/Interfaces/LAN/Port table.

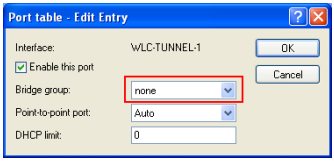


Figure 57: Port settings for public-spot APs

- For the guest Internet access, create an entry in the list of DSL remote terminals with the short hold time ‘9999’ and the pre-defined layer ‘DHCPOE’. The value ‘9999’ sets up a connection immediately without a time restriction. This example requires that a router with activated DHCP server provides the Internet access. In LANconfig, you can find this setting under Configuration/Communication/Remote terminals/Remote terminals (DSL)

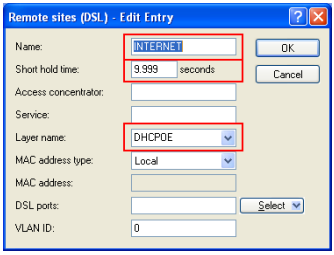


Figure 58: Remote terminal for Internet access

- For internal use, create the IP network 'INTRANET', e.g. with the IP address '192.168.1.100' and the interface tag '1', for guest use, create the IP network 'GUEST ACCESS', e.g. with the IP address '192.168.200.1' and the interface tag '2'. The virtual router in the WLAN Controller uses the interface tags to separate the routes for the two networks. In LANconfig, you can find these settings under Configuration/IPv4/General/IP networks.

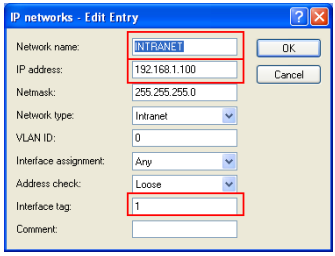


Figure 59: IP network for internal use

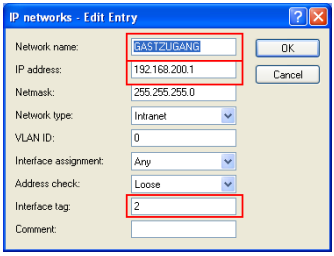


Figure 60: IP network for guest access

- The WLAN Controller can function as DHCP server for the Access Points and the WLAN Clients logged in. For this purpose, enable the DHCP server for the 'INTRANET' and the 'GUEST ACCESS'. In LANconfig, you can find this setting under Configuration/IPv4/DHCPv4/DHCP networks.

  Note: The activation of the DHCP server is obligatory for the guest network, optional for the internal network. You can implement the DHCP server for the internal network differently.

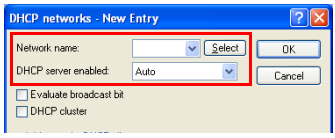


Figure 61: DHCP network for guest access

- Create a new standard route in the routing table which forwards the data from the guest network to the Internet access of the WLAN Controller. Select routing tag '2' and the 'Internet' router. Also activate the option 'Mask Intranet and DMZ (standard)'. In LANconfig, you can find this setting under Configuration/IP router/Routing/IPv4 routing table.

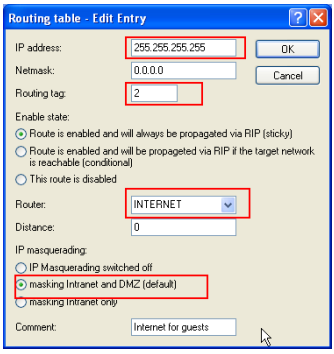


Figure 62: Routing entry for Internet access

- Activate the public-spot login for the logical LAN interface 'WLC-tunnel-1'. In LANconfig, you can find this setting under Configuration/Public spot/ Public spot.

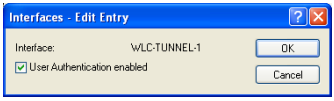


Figure 63: Activating the user login for the WLC tunnel

- As the last step, activate the option "Authenticate with name and password" via the public spot for the WLAN Controller. In LANconfig, you can find this setting under Configuration/Public spot/Login.

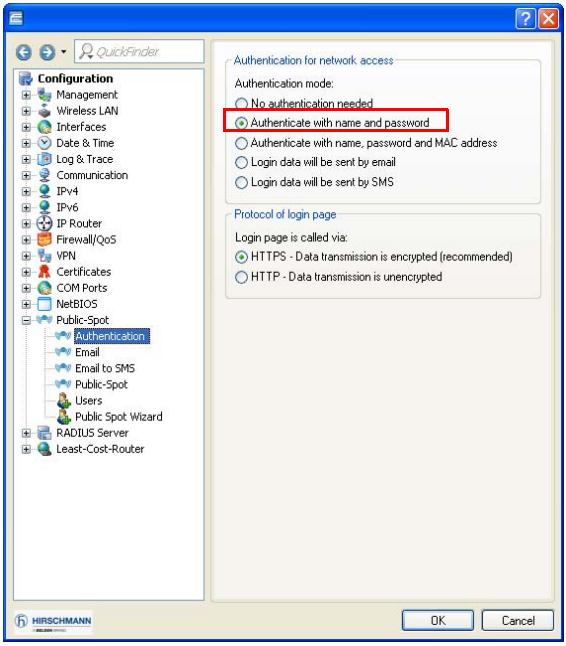


Figure 64: Activating the login via the public spot

Apart from the configuration of the WLAN Controller, you can configure the public spot to meet your requirements, either for the use of an internal or an external RADIUS server.

5 Public Spot

5.1 What is a Public Spot?

Public Spots, also called hotspots, are places where users can connect their terminals ? such as smartphones, tablet PCs or laptops ? to a publicly accessible network. Normally, these networks provide connections to the Internet; however a Public Spot can also be limited to a local network in order to offer extra information to users visiting a museum or a trade show, for example. The term is usually synonymous to the devices with which the user can connect to the network, which is also why this manual does not differentiate between the location and the device.

Although Public Spot access via wireless LAN is widespread, access via a cabled LAN connection is also possible. The most popular demand for these services originally came from business travelers at airports, in hotels, or at other locations where their end devices require access to online content. The public rarely has access to modems, ISDN or broadband connections in areas like this. However, the recreational use of Public Spots by private persons has become very popular.

5.1.1 The Solution: (W)LAN Technology

Public Spot scenarios make use of the widespread (W)LAN technologies based on the internationally established IEEE 802.11/802.3 standards:

- Access via WLANs provides fast, uncomplicated network access by radio. The user only needs a WLAN adapter for their mobile device, which, for modern devices, is usually part of the standard equipment or can be inexpensively added, usually with a USB interface. The bandwidth is sufficient for most applications, even when multiple users are simultaneously logged in to a Public Spot.
- With automatic address allocation via DHCP, access via LAN is similarly uncomplicated: In this case, the user only needs a LAN adapter and a suitable cable for their end device, in order to connect their device to the Public Spot network at a wall socket.

However, when accessing via LAN the user loses mobility and uninterrupted flexibility. However, this access ? assuming that a corresponding infrastructure is available ? also provides stable network operation with the highest network load (for example, for multimedia content such as video-on-demand) and a higher number of users (for example, in a large hotel), where connections via WLAN may reach their limits sooner. It is also possible to add a Public Spot offering to an existing cable infrastructure (for example, in a college) with the use of a Public Spot via LAN.

Special Considerations for Access via (W)LAN

It is difficult to employ a standard WLAN access point or LAN router as a Public Spot for two main reasons:

- User authentication is only possible by employing RADIUS/802.11x, so requiring the appropriate infrastructure and configuration.
- There is no facility for billing / accounting.

For this reason, the use of devices without the Public Spot function is not practical, since these devices are not able to separate and log the specific network usage of authorized and unauthorized users of publicly accessible networks.

5.1.2 User Authorization and Authentication

As soon as an end device moves within range of an access point, the user can spontaneously established a connection to this access point. The same is true for open LAN connections. However, the problem is that access should not be available to the public in general, but only to certain selected users. Setting up restrictions of this type is the task of a Public Spot.

For this purpose, a Public Spot must be in a position to control access to the WLAN on a user basis. For simple Public Spot installations, user data can be locally stored and managed in the router or access point ? or alternatively on a WLAN controller. Instead, complex installations employ a direct database connection to a central authentication server in the interests of detailed accounting or direct management. Central servers of this type generally work with RADIUS technology.

5.1.3 Accounting

If the Public Spot operator does not want to offer this service free of charge, connection data has to be collected and billed for each user. Typical methods include: Purchase of a limited amount of online time (pre-paid method), retrospective payment of consumed resources (credit payment), or unrestricted access until a certain time (e.g. checking out of a hotel).

For smaller Public Spot installations, accounting functions should be as simple as possible, and they should be implemented locally in the device. Larger installations offer the facilities for billing via an external RADIUS server.

5.1.4 Logging

The operation of commercial telecommunications services is subject to national regulations. Certain information is to be recorded and presented to law enforcement agencies upon request.

The Public Spot module provides suitable functions for recording user data with RADIUS accounting and SYSLOG.

Hinweis: Please note that operating a Public Spot (also referred to as a hotspot) can be subject to legal regulations in your country. Before installing a Public Spot, please inform yourself about any applicable regulations.

5.2 Overview of the Public Spot Module

The demands placed on devices operating Public Spots are as varied as the environments they are employed in. A Public Spot offers various functions which are described in more detail in the following sections.

5.2.1 Open User Authentication (OUA)

Open User Authentication (OUA) is a method for web-based authentication via a form. This makes it ideal for Public Spot installations.

Typical Procedure for an Online Session with OUA

☐ The user of a W(LAN)-enabled end device is within range of an access point or a network outlet in Public Spot mode. Internet access or the use of chargeable services is not yet available at this phase.

- WLAN: After system startup, the WLAN adapter automatically logs on to the appropriate access point.
- LAN: After system startup the user connects to the network with a suitable cable and is assigned an address by the DHCP server.

☐ The user starts a web browser. The device offering the Public Spot service automatically directs the user to the login page of the Public Spot. This page provides detailed information on using the services.

Generally, the user purchases a voucher with login data that grants a limited amount of access time. Other login methods are also possible, such as independently requesting login data via e-mail or text message (SMS).

☐ In the case of a login using a voucher, the user enters his login data (username and password) on the login page. Depending on the configuration, the RADIUS server on the device (internal) or an external one checks the login data that was entered. If the login is successful, the user gains access to the Public Spot. Otherwise an error message will be displayed. If a prepaid model is employed, i.e. access is to be granted for a limited period of time only, then the RADIUS server additionally informs the Public Spot about the user's time credit.

☐ The user can log off from the Public Spot at any time. The Public Spot can terminate a session itself if the time credit has expired, if a specified expiry date is reached, or if contact is lost for an extended period.

During and at the end of a session the Public Spot provides the user with an overview of the session data. If required, the Public Spot can simultaneously transmit all important accounting information to the RADIUS server. This can be the device's internal server or an external server.

OUA can be Employed Universally

The big advantage of the OUA method is that it is completely based on standard protocols. This guarantees that OUA can be operated universally. It works with any (W)LAN adapter, can be seamlessly integrated in existing network infrastructures, and makes it possible to implement additional features, for example, when the WLAN is between cells during roaming.

5.2.2 Security in the (W)LAN

Wireless LANs are potentially a significant security risk. Public Spots present similar risks to the operator and users.

Security for the Operator

Operators of Public Spots are primarily interested in the security of their own network infrastructure. The Public Spot module provides operators with a range of security technologies and methods:

- **Multi-SSID** (only WLAN)**, VLAN and virtual routers**
  - The safe separation of public access can be achieved using one or more different radio cells for an access point (Multi-SSID).
  - VLAN technology can separate public access from the private network of the operator.
  - Virtual routing technology ARF (Advanced Routing and Forwarding) supplies one SSID with its own security and QoS settings and only specific destinations are routed on it.

  This ensures that guest access over a Public Spot is securely and effectively separated from the productive network, even though they share the same infrastructure. The device's internal firewall can, for example, limit the available bandwidth in the WAN to max. 50?%, and access can be restricted to web pages (HTTP, port?80) and name resolutions (UDP?53).

- **Traffic limit**

To avoid denial-of-service (DoS) and brute-force attacks on the Public Spot you can restrict the permissible data transfer for non-authenticated Public Spot users to a harmless volume.

- **Locking access to the configuration**

  You can lock access from your Public Spot network to device configurations (e.g., your access points, WLAN controllers or routers) so that access to configurations is only possible using other specific management interfaces.

Security for the User

The primary security concern for users of Public Spots is the confidentiality of their data. Users are also interested in security of user data to avoid misuse. Users are protected by the following security technologies:

- **Intra-cell blocking** (WLAN Only)

  Prevent communication between the WLAN clients in your Public Spot network. Along with the user's existing security mechanisms, this measure helps to prevent unauthorized access to the resources of your Public Spot users.

- **Encryption during the login phase**

  If you have a digital certificate, you can load it on your device in order to secure usernames and passwords using an encrypted HTTPS method. The digital certificate should be signed by a recognized public authority so that browsers classify it as trustworthy and do not display security errors to the users. If there is no certificate, data is sent unencrypted.

Hinweis: The certificate merely secures the login process, as the data within a Public Spot network are normally not encrypted. This is true for LAN as well as WLAN connections. If your users wish to secure their regular data traffic as well, they will have to use their own encryption methods.

▶An exception to this are the WLAN connections via HotSpot?2.0: Since the HotSpot 2.0 standard is based on WPA2 (802.1X/802.11i), EAP and 802.11u, data packets are always encrypted for transmission, both for authentication and during the session.

Hirschmann strongly recommends that sensitive user data should only ever be transferred via encrypted connections, such as IPSec-based VPN tunnels or HTTPS encrypted data connections. In addition to this, Public Spot users should ensure that a personal firewall is active on their end devices.

5.2.3 Setup Wizard for Public Spots

The „Setup Public Spot“ wizard helps you to setup and perform the initial configuration of your Public Spot. You can set up a functional Public Spot network with just a few clicks. The wizard groups the necessary settings together (e.g. assign an interface, choose an IP range, specify the access format and login procedure, logging) and offers you the option to create an administrator with limited rights who can only create and manage Public Spot users.

5.2.4 Wizard for Managing Users

Using the setup wizard „Create Public Spot account“ you can use WEBconfig to create temporary accesses to the Public Spot network with just a few clicks of the mouse. In the simplest case, you only need to enter the duration of access, the wizard assigns the username and password automatically and stores the credentials in the user database of the internal RADIUS server. The user receives a printed, personalized voucher, which the user can use to login to the Public Spot network for the specified period.

5.3 Basic Configuration

The instructions for the basic settings are divided into several separate sections:

- The first section describes the setup of an operational Public Spot using a wireless router as an example.

  Hinweis: To set up a Public Spot for a simple application scenario, you can start the corresponding wizard, which assists you in configuring the Public Spot.

- The second section describes the configuration of the default values for the user wizard with which new employees can easily create and manage new Public Spot users without the need for general administrator rights. This also includes creating a limited access account with which your employees can access this wizard only.
- The third section describes user administration on the local RADIUS server with LANconfig.

To a certain extent these sections are dependent on one another, and ideally you should work through them in sequence.

5.3.1 Basic installation of a Public Spot for Simple Scenarios

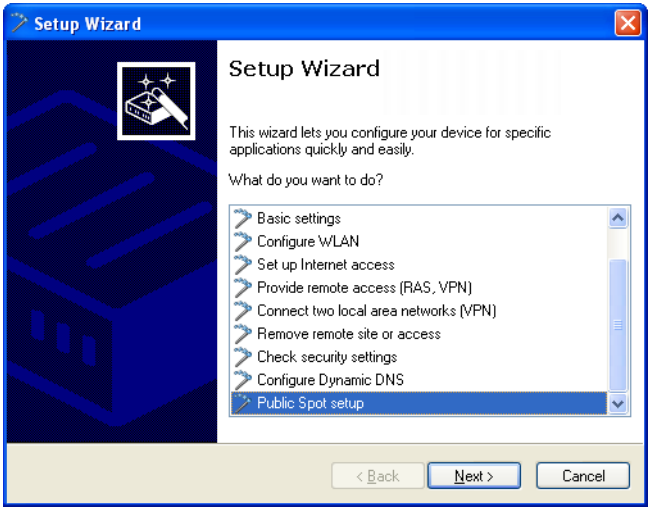
Installation Using the Setup Wizards

The following tutorial describes how to use LANconfig's Public Spot setup wizard to perform a basic Public Spot installation.

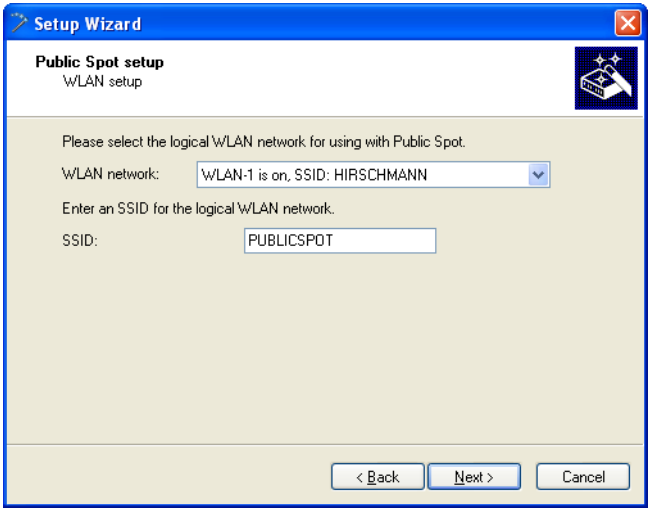
Hinweis: The wizard for the basic configuration of the Public Spot shows different dialogs depending on the device type and your previous choices. This tutorial is only an example.

☐ To do this, start LANconfig and select the device for which you want to set up the Public Spot.

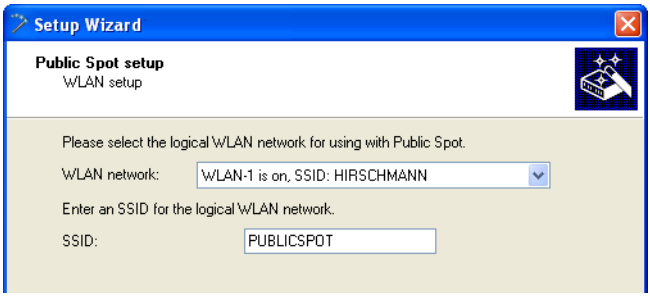
☐ Start the Setup Wizard with `Device:Setup wizard`, select the action „Setup Public Spot “and then click „Next“.


Setup Wizard
Setup Wizard
This wizard lets you configure your device for specific applications quickly and easily.
What do you want to do?
Basic settings
Configure WLAN
Set up Internet access
Provide remote access (RAS, VPN)
Connect two local area networks (VPN)
Remove remote site or access
Check security settings
Configure Dynamic DNS
Public Spot setup
< Back
Next >
Cancel

☐ If you want the Public Spot to be available over WLAN, enable the corresponding option and select the physical WLAN module to be used to operate the Public Spot. Click „Next“.



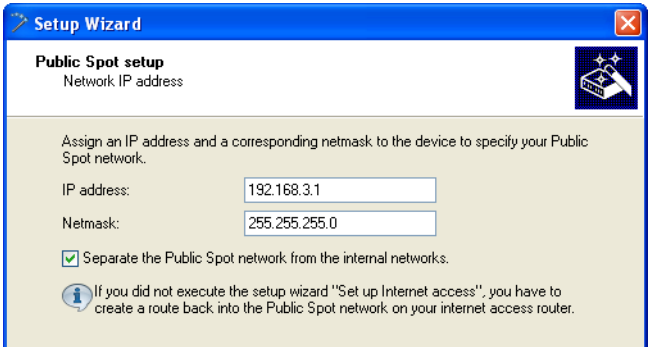
☐ Select the logical interface from the drop-down menu which the Public Spot should offer (e.g., WLAN-1), and enter a descriptive name for the wireless network (SSID). Click „Next“.



☐ Assign the IP address and netmask to the device that your Public Spot network should specify and click „Next“.

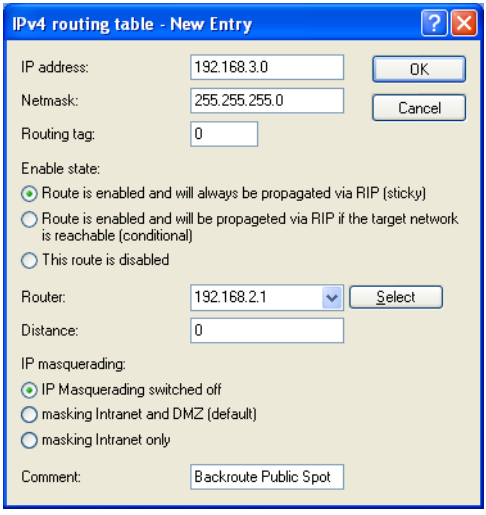
The Public Spot module has its own address on your network, which is independent from the address that you assigned to your device. For example, if you have a 192.168.0.0/24 network set up and your device has the IP address 192.168.2.1, you can assign the IP address `192.168.3.1` and the subnet mask `255.255.255.0`, as long as this IP address has not already been used elsewhere.

If you want to separate the Public Spot network from internal networks for security reasons, make sure that the corresponding option is enabled.


Setup Wizard
Public Spot setup
Network IP address
Assign an IP address and a corresponding netmask to the device to specify your Public Spot network.
IP address:
192.168.3.1
Netmask:
255.255.255.0
Separate the Public Spot network from the internal networks.
If you did not execute the setup wizard "Set up Internet access", you have to create a route back into the Public Spot network on your internet access router.

Hinweis: If your device is not directly connected to the Internet and you have a different address range for your Public Spot, you must set up a return route to your Public Spot network on your Internet gateway. If there is no return route, Public Spot users will see an HTTP error after they have successfully authenticated.

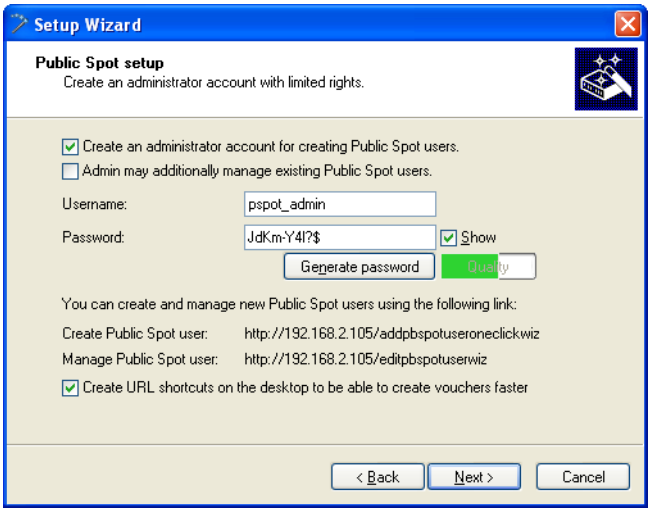
Please find the directions on how to set up a return route in the documentation for your Internet gateway. If it is a OpenBAT device, you can configure it under `IP router:Routing:IPv4 routing table`. To do this, create a new entry and enter the network address of your Public Spot network under „IP Address“ and under „Router“ enter the address of the Public Spot in your local network.



☐ If necessary, create an administrator with limited rights who can use the setup wizards in WEBconfig to create Public Spot users. To continue, click on „Next“.

This type of administrator is useful when you want your employees to be able to manage user accounts themselves without the help of a device administrator. The right to create new accounts in WEBconfig enables the Create Public Spot account wizard, and administrator rights enable the Manage Public Spot account wizard.

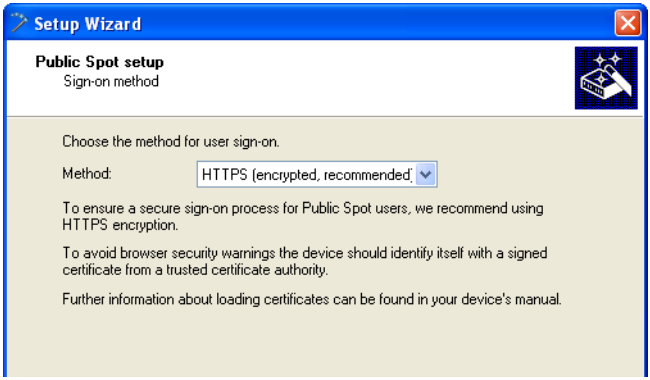
Using the user creation wizard „Create Public Spot account“, the administrator has the option of creating time-limited accounts for Public Spot users and print the corresponding login data on a voucher.


Setup Wizard
Public Spot setup
Create an administrator account with limited rights.
Create an administrator account for creating Public Spot users.
Admin may additionally manage existing Public Spot users.
Username:
pspot_admin
Password:
JdKm-Y4l?$
Show
Generate password
You can create and manage new Public Spot users using the following link:
Create Public Spot user:
http://192.168.2.105/addpbspotuseroneclickwiz
Manage Public Spot user:
http://192.168.2.105/editpbspotuserwiz
Create URL shortcuts on the desktop to be able to create vouchers faster
< Back
Next >
Cancel

Hinweis: Make sure that the password you create is secure. The Setup Wizard will check the quality of the password you enter. For passwords that are not secure the input field appears in red, when it is more secure it changes to yellow, and when it is very secure the background turns green.

☐ Select the procedure for user login. To continue, click on „Next“.

You can select „HTTPS“ or „HTTP“ in the drop-down list. Using a connection with HTTPS provides a secure connection for Public Spot users.


Setup Wizard
Public Spot setup
Sign-on method
Choose the method for user sign-on.
Method:
HTTPS (encrypted, recommended)
To ensure a secure sign-on process for Public Spot users, we recommend using HTTPS encryption.
To avoid browser security warnings the device should identify itself with a signed certificate from a trusted certificate authority.
Further information about loading certificates can be found in your device's manual.

☐ The click „Next“ and finally „Finish“ to complete the basic installation of the Public Spot. The Setup Wizard will now send the settings to the device.

That's it! You have completed configuration of your Public Spot module! Now, if you come within range of a Public Spot with a WLAN-capable device, the device can find the SSID that you set up as a public network and login to it.

Manual Installation

The following configuration steps show you how to manually setup a Public Spot for simple scenarios. For the application scenario described here, you enable the Public Spot on an interface over which there is no other data traffic other than the Public Spot traffic ? where Public Spot and normal WLAN users do not share the same network (dedicated SSID).

Hinweis: This tutorial is only an example. Depending on the device type (access point, WLAN controller, etc.) or complexity of the network configuration (e.g., use of VLAN or ARF), different or additional steps may be required for setting up a Public Spot. Since this type of network configuration can be highly customized, this tutorial concentrates specifically on a simple example, so that you can adapt the steps as needed.

☐ To do this, start LANconfig and select the device for which you want to set up the Public Spot. Next, open the configuration menu for the device.

☐ Check that the time is correct.

It is important for the Public Spot to be set with the right time in order to check the certificates and correctly record and bill session data. First make settings such as time zone and time changes (summer and standard time):

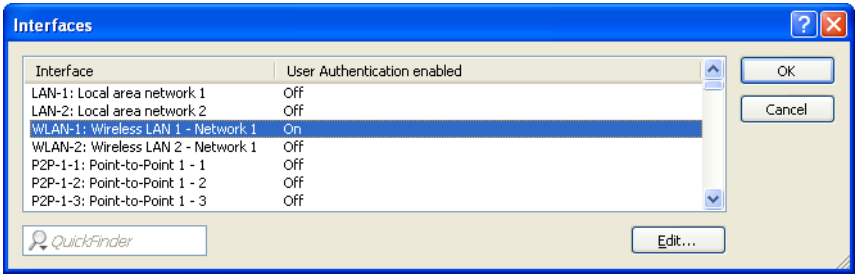
▶ LANconfig: `Date/Time:General`

Hinweis: In order to ensure that the time of the Public Spot remains correct, the device should be set up as an NTP client. Enter the time server that is necessary for that under `Date/Time:Synchronization:Time server`. Open the "Add" window to show a list of possible server addresses.

☐ Select the interfaces for the Public Spot operation.

Here you activate the interfaces which will be available to registered users. Along with the logical WLAN interfaces which Public Spot users directly login to, the logical LAN interfaces (LAN-1, etc.), and the point-to-point connections (P2P-1, etc.) can also be selected. When connected via the LAN or P2P interface, you can integrate additional access points into the Public Spot of a OpenBAT device. For an access point select, for example, the logical WLAN interface „WLAN-1“ of WLAN module 1.

▶ LANconfig: `Public-Spot:Public-Spot:Interfaces`



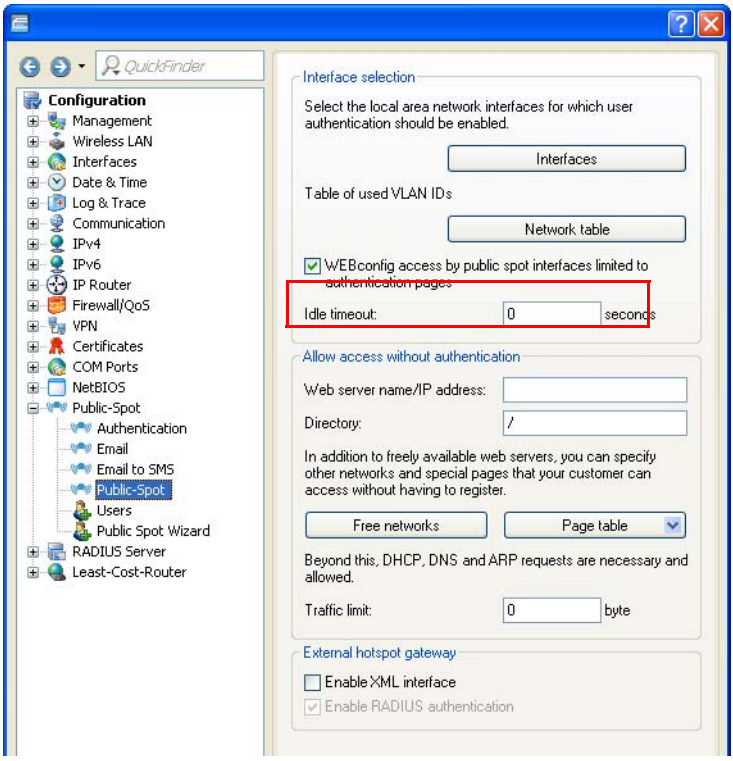
By activating the authentication for a WLAN interface, you automatically release the associated SSID for the Public Spot operation.

Hinweis: On a BAT controller you can enable certain Ethernet interfaces for the Public Spot. In this manner you can also set up selective restrictions for certain VLANs.

☐ Access to your device from the Public Spot network should be restricted to the authentication pages.

If you do not restrict access, Public Spot users will be able to access the configuration interface of your device (WEBconfig). For security reasons you should not permit this.

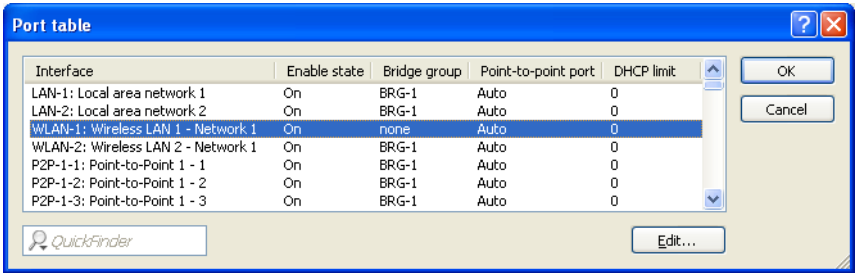
- LANconfig: `Public Spot:Public Spot:WEBconfig access by Public Spot interfaces limited to authentication pages`



☐ Disconnect the interface which is to be used for Public Spot operations from the other network traffic.

In order for end devices to be able to communicate with each other using different interfaces of a OpenBAT device (e.g., between LAN-1 and WLAN-1), these interfaces are logically connected to each other (bridged) within your device. However, in a Public Spot scenario this type of bridging may not be desirable for security reasons. In order to disconnect the communication between an interface (e.g., WLAN-1) assigned to a Public Spot and the rest of the network, you have to remove bridging. In the „Port table“ set the „Bridge group“ for the respective interface to `none`.

▶ LANconfig: `Interfaces:LAN:Port table`

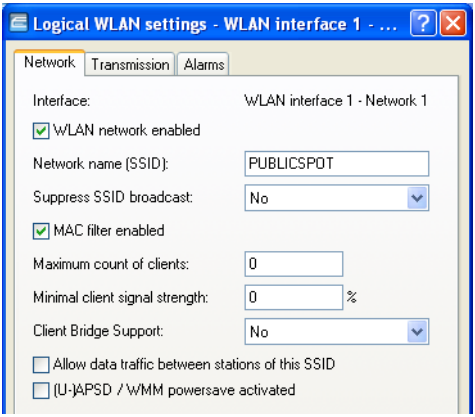

Port table
Interface
Enable state
Bridge group
Point-to-point port
DHCP limit
LAN-1: Local area network 1 On BRG-1 Auto 0
LAN-2: Local area network 2 On BRG-1 Auto 0
WLAN-1: Wireless LAN 1 - Network 1 On none Auto 0
WLAN-2: Wireless LAN 2 - Network 1 On BRG-1 Auto 0
P2P-1-1: Point-to-Point 1 - 1 On BRG-1 Auto 0
P2P-1-2: Point-to-Point 1 - 2 On BRG-1 Auto 0
P2P-1-3: Point-to-Point 1 - 3 On BRG-1 Auto 0
OK
Cancel
QuickFinder
Edit...

☐ Enable the WLAN for the Public Spot.

This setting does not affect: BAT-Controller.

Activate the logical WLAN which you enabled for the Public Spot login and assign a descriptive name to this network (SSID).

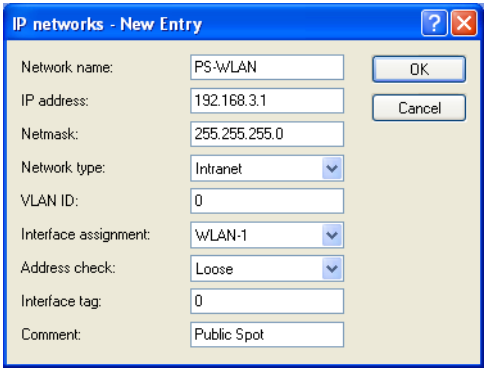
- LANconfig: `Wireless LAN:General:Interfaces:Logical WLAN settings:WLAN interface <number> - Network <number>:Network`



☐ Assign the IP address and netmask to the device that your Public Spot network should specify.

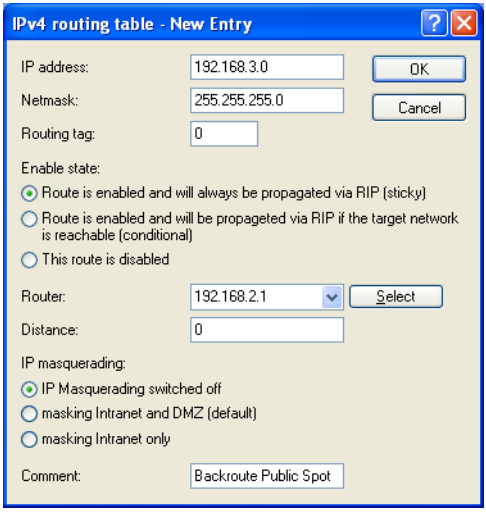
The Public Spot module has its own address on your network, which is independent from the address that you assigned to your device. For example, if you have a 192.168.0.0/24 network set up and your device has the IP address 192.168.2.1, you can assign the IP address `192.168.3.1` and the subnet mask `255.255.255.0`, as long as this IP address has not already been used elsewhere. Select the interface that you chose under „Interface assignment“ e.g., `WLAN-1`.

- LANconfig: `IPv4:General:IP networks`



Hinweis: If your device is not directly connected to the Internet and you have a different address range for your Public Spot, you **must** set up a return route to your Public Spot network on your Internet gateway. If there is no return route, Public Spot users will see an HTTP error after they have successfully authenticated.

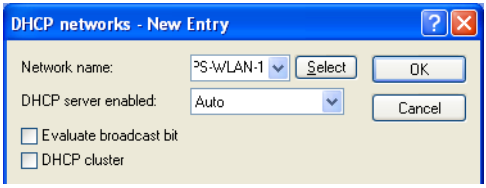
Please find the directions on how to set up a return route in the documentation for your Internet gateway. If it is a OpenBAT device, you can configure it under `IP router:Routing:IPv4 routing table`. To do this, create a new entry and enter the network address of your Public Spot network under „IP Address“ and under „Router“ enter the address of the Public Spot in your local network.



☐ Configure the DHCP server settings for the Public Spot network.

Since the device has an IP network that is independent from the network where it is located, you must configure a DHCP server for this network. For the previously set up IP network (e.g., `PS-WLAN-1`), set the value for „DHCP server enabled“ to `automatic`.

▶ LANconfig: `IPv4:DHCPv4:DHCP networks`

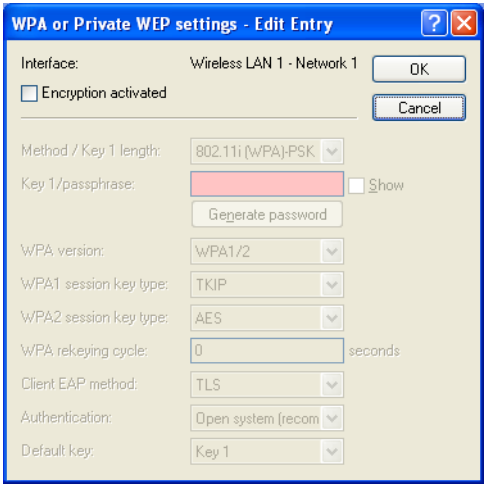


☐ Disable the encryption for the interface that you are using for the Public Spot.

This setting does not affect: BAT-Controller.

Encryption for all logical WLANs is enabled by default. In Public Spot applications, the payload data between the WLAN clients and the access point are usually transmitted unencrypted. For this reason, disable encryption for the logical WLAN which you previously set up for the Public Spot login.

- LANconfig: `Wireless-LAN:802.11i/WEP:WPA or Private WEP settings`

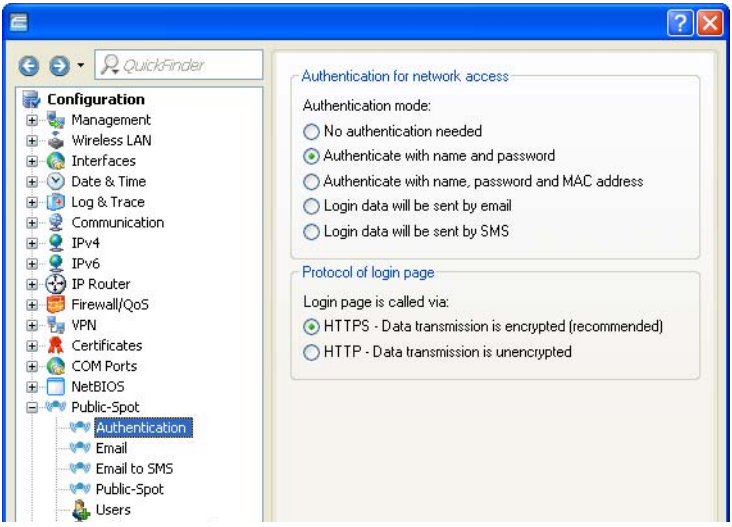


☐ Select the authentication mode and the protocol used for the user login.

The authentication method that you select determines the information which users of the Public Spot WLAN must enter when logging in. Select „Authenticate with name and password“ to allow your users the option to login with an individual username and password that you have previously assigned them. This setting also allows you to quickly provide hotspot access to your guests using vouchers (tickets).

Use „HTTPS“ as the protocol in order to be able to send encrypted login data to your users during login.

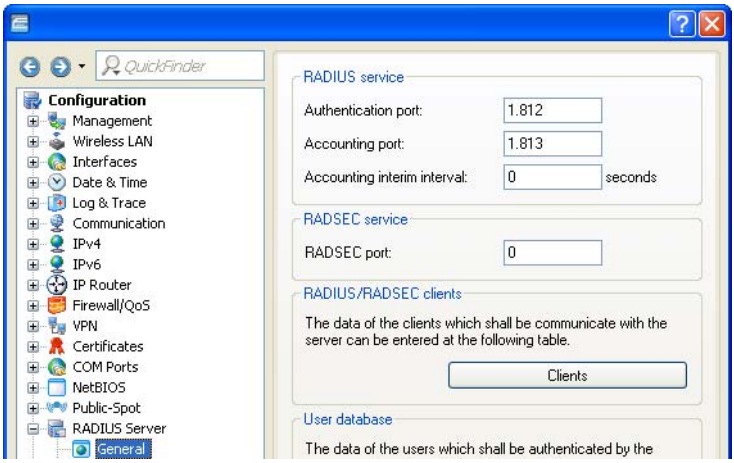
▶ LANconfig: `Public Spot:Authentication:Authentication mode`



☐ Specify the internal RADIUS server as the server responsible for user administration and accounting. To do this, enter the „Authentication port“`1812` and „Accounting port“`1813`.

You store Public Spot access accounts in the user database on the device's own RADIUS server. In order to use Public Spot access accounts, you **must** configure the RADIUS server and, in the following step, the Public Spot module to use the RADIUS server.

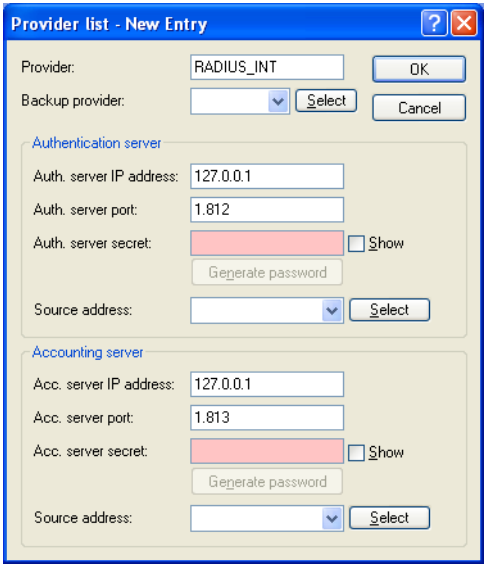
▶ LANconfig: `RADIUS server:General`



☐ Create an entry for the internal RADIUS server in the list of authentication servers of the Public Spot. Under „Auth. server IP address“ and „Acc. server IP address“ enter the loopback address `127.0.0.1`. Use the „Auth. server port“ and „Acc. server port“ used for the authentication port and accounting port in the previous settings.

The list entry is necessary in order for the Public Spot to recognize the address of the RADIUS server and so that it can authenticate Public Spot access on the internal RADIUS server.

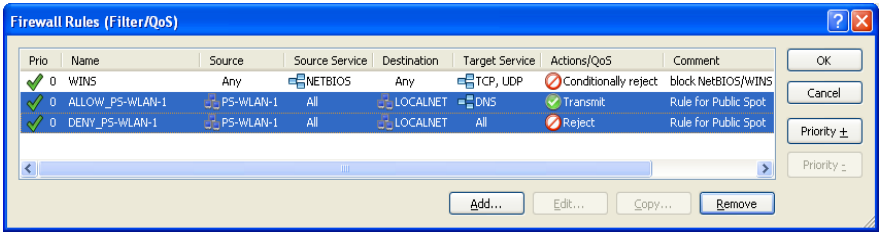
▶ LANconfig: `Public Spot:Users:Authentication servers`

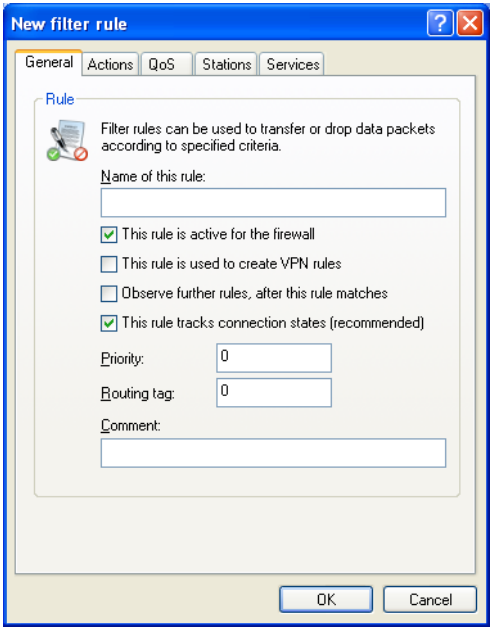


☐ Set up filter rules in the Public Spot's firewall to secure your local network. In each case, create an "accept" rule (for example, `ALLOW_PS-WLAN-1`) and a "reject" rule (for example, `DENY_PS-WLAN-1`).

You use the accept rule when devices are to be able to send DNS requests from the Public Spot network to all local networks, e.g., your local intranet. On the other hand, with a reject rule you generally block all access or requests from the Public Spot network to your local network. The order ? accept before reject ? is essential, since the firewall applies rules from top to bottom of the list.

- LANconfig: `Firewall/QoS:IPv4 Rules:Rules?`





Settings for the Accept Rule:

- Enter the name of the rule in „General“, for example, `ALLOW_PS-WLAN-1`.
- Remove all possible predefined action objects from the list and using `Actions:Add...` add an action object of type „ACCEPT“.
- In `Stations:Connection source`, enable the option „Connections from the following stations“ and select `Add...:Add custom station`.
- In the Stations window that opens, select the option „All stations in local network“ and for „Network name“ select the name of your Public Spot IP network, e.g., `PS-WLAN-1`. Close the dialog with „OK“.
- In `Stations:Connection destination`, enable the option „Connections to the following stations“ and after selecting „Add...“ choose „LOCALNET“.
- In `Services:Protocol/target services` enable the option „Following protocol/target services“ and select `Add...:DNS`.
- End the filter rule dialog with a final click on „OK“.

LANconfig then enters the allow rule into the rule table.

Settings for the Reject Rule:

- Enter the name of the rule in „General“, for example, `DENY_PS-WLAN-1`.
- Remove all possible predefined action objects from the list and using `Actions:Add...` add an action object of type „REJECT“.
- In `Stations:Connection source`, enable the option „Connections from the following stations“ and select `Add...:Add custom station`.

- In the Stations window that opens, select the option „All stations in local network“ and for „Network name“ select the name of your Public Spot IP network, e.g., `PS-WLAN-1`. Close the dialog with „OK“.
- In `Stations:Connection destination`, enable the option „Connections to the following stations“ and after selecting „Add...“ choose „LOCALNET“.
- End the filter rule dialog with a final click on „OK“.

LANconfig then enters the rejection rule in the rule table.

☐ Store the configuration on your device.

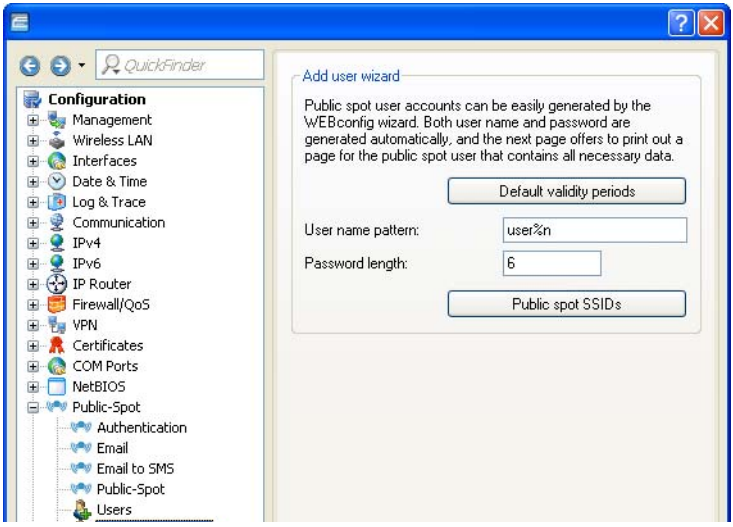
That's it! You have completed configuration of your Public Spot module! Now, if you come within range of a Public Spot with a WLAN-capable device, the device can find the SSID that you set up as a public network and login to it.

5.3.2 Default Values for the Public Spot Wizard

The following section describes how you define default values for the new-user wizard („Create Public Spot account“).

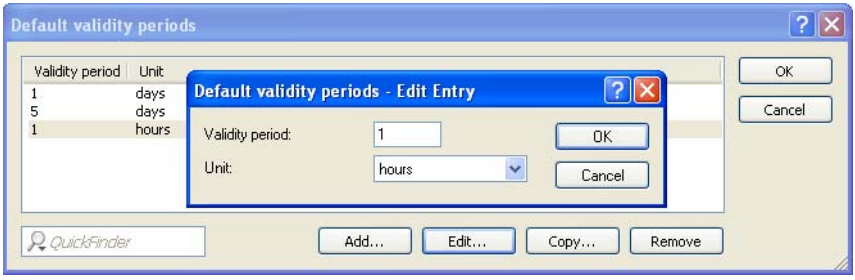
☐ Start LANconfig and open the configuration dialog for the device.

☐ Change the view to `Public Spot:Public Spot Wizard`.



☐ In „Default validity periods“, define which default validity periods for user accounts and vouchers are to be available by default.

The new-user wizard takes the shortest validity period as the default.



☐ In „User name pattern“ you indicate what pattern is used by the new user wizard to create usernames.

You can enter up to 19 characters, whereby the wizard will automatically create a unique number for every user if you enter "%n". The default description `user%n` will be shown later on the voucher, for example, as `user12345`.

☐ Using „Password length“ you specify the length of the passwords that the new user wizard generates for Public Spot access.

The default is 6 characters. If you would like to have longer passwords, keep in mind that guests can make mistakes when entering them, which can cause unnecessary problems and complaints.

5.3.3 Setting up an Administrator for Public Spot Management

In order for employees to be able to manage a Public Spot on the device without further permissions, you can explicitly assign them the function rights to use the Public Spot wizard. This tutorial describes the steps to set up Public Spot function rights for employees without giving them additional administrator rights.

Hinweis: You need to have the "Supervisor" permission to be able to assign Public Spot management to an employee.

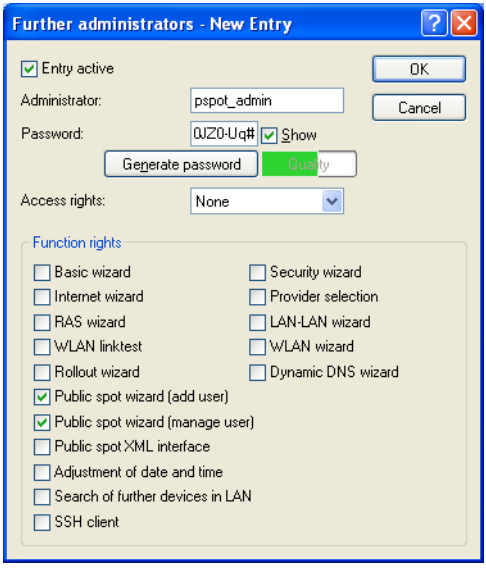
☐ Start LANconfig.

☐ Open the configuration for the device for which you want to register a Public Spot administrator.

The Public Spot option has to be enabled on this device.

☐ Change to the view `Management:Admin`, click in the section „Device configuration“ on „Further administrators“, and then click on „Add“.

If you want to allow an existing user to perform Public Spot management, select the user's entry in the table and click on „Change“.



☐ You activate the profile by checking the „Entry enabled“ box.

☐ Assign a descriptive name in the field „Administrator“.

☐ Enter a „password“ and repeat it to be sure.

☐ Set the „Access rights“ to „None“.

When you modify an existing user, you should not modify existing function rights.

☐ In the section „Function rights“ enable the „Public Spot wizard (add user)“, and „Public Spot wizard (manage user)“.

When you modify an existing user, you should not modify existing function rights.

☐ Save the new or modified profile by clicking on „OK“.

The Public Spot administrator is offered the Public-Spot wizards in the navigation when they log on using WEBconfig.

Using the user creation wizard „Create Public Spot account“, the administrator has the option of creating time-limited accounts for Public Spot users and print the corresponding login data on a voucher.

Hinweis: The function right „Public Spot XML interface“ is not needed by a normal Public Spot admin. The right is only relevant if you use the XML interface (see page 362), and should not be combined with the function rights described above for security reasons.

5.3.4 Setting up Public Spot users for Simple Scenarios

You can set up Public Spot users either manually or by using the setup wizard. Setting up the configuration options manually offers you more extensive options and allows you, for example, to create self-defined users with an unlimited lifetime.

On the other hand, the setup wizard allows you to create generic Public Spot users with automatically generated login data with limited lifetimes. The respective setup wizard is only accessible using WEBconfig, which allows you to quickly create users without requiring administrator permissions for the entire device. The only requirement is an administrator with limited permissions.

You naturally also have the option to initially create generic users with the aid of the setup wizard and then manually adapt them to your needs (e.g., change the usernames).

- **Adding Public Spot Users with a Single Click and Voucher Printing**

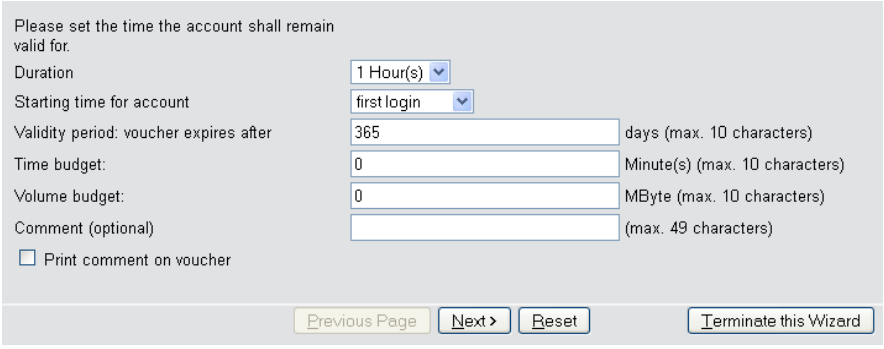
  The following section describes the setup of a Public Spot user using WEBconfig and then printing a voucher. You can also prepare vouchers in advance.

Hinweis: You need the permissions for the „Public Spot Wizard“, in order to create a new Public Spot user.

☐ Log on to the WEBconfig home page as an Administrator.

☐ Start the setup wizard by clicking on `Setup wizards:Create Public Spot account`

☐ The new user wizard starts with an input screen. The fields have default values.



The wizard automatically creates a username and a password. In the subsequent printout dialog you can select the voucher printer and print-out the voucher.

☐ If necessary, you can change the default values before you print it.

The following entries affect the appearance as well as the validity of the vouchers:

- „Duration“: Set how long access is to be available after registration or the first login. The values listed here are managed in the „Default validity periods“ table. The pre-defined values are:

  `1 Hour(s)`

  `1 Day(s)`

  `5 Day(s)`

- „Starting time for access“: Sets the time when the voucher becomes valid. Possible values are:

  `First login`: Access is valid as of the user's initial login

  `Immediately`: Access is valid as of the creation of the user's account

  To a supply of vouchers in advance, select `First login` as the validity of the vouchers. That way the vouchers will still be valid even after a longer period.

- „Validity: Voucher expires after“: Enter the period after which the voucher becomes invalid. If the access is to be valid immediately, it is not possible to enter a validity period.

- „Time budget (minutes)“: Specify the amount of time after which access to the Public Spot is closed. Depending on the chosen expiry method, access time is limited either to the time budget (incremental) or to the set voucher validity period (absolute).

- „Volume budget (MByte)“: Specify the available data volume after which access is closed.

- „Comment (optional)“: Enter a comment here. This comment can contain, for example, additional notes about the access duration or the telephone number of the receptionist in case of access problems.

- „Print comment on voucher“: Check this option if the comment is to appear on the voucher.

☐ Click „Next “and finally „Save and print out user data“ to create the new user account and print out a voucher.

Manual Setup and Management

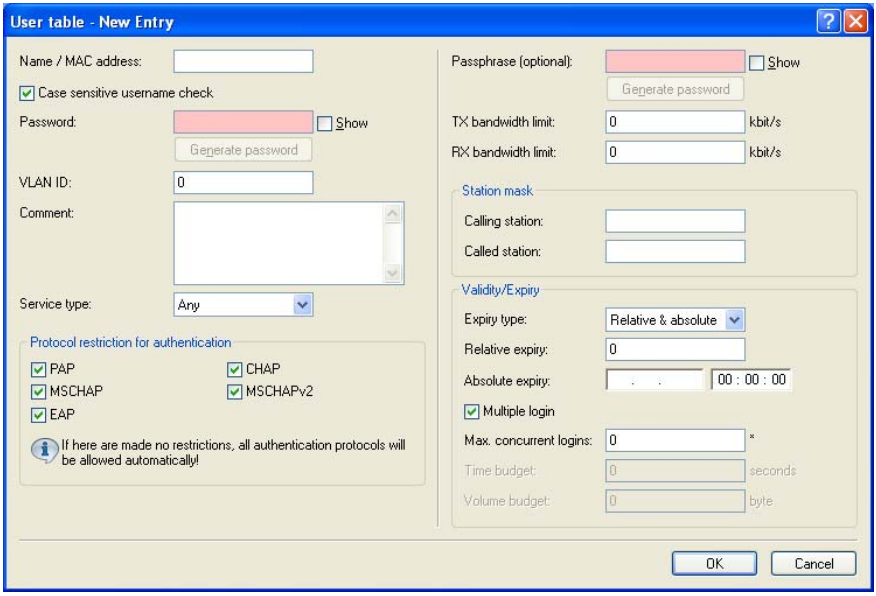
The following configuration steps show you how to use LANconfig to manually setup a Public Spot user for simple scenarios. You create and manage Public Spot users using the „User database“ in the internal RADIUS server of the device under `RADIUS server:General`. This is where you ? and also the setup wizard ? enter all of the users who should have access to the Public Spot.

Hinweis: For user administration, the Public Spot module also has its own internal list (found under `Public Spot:Users:User list`). During technical development, this list was replaced as of HiLCOS?7.70 by the user administration via RADIUS. For compatibility reasons, the device still evaluates the internal user list of the Public Spot module if it is enabled. However, for a new installation you should no longer use this list, since it prevents you from using many features (setup using the wizard, bandwidth restrictions, accounting via RADIUS, VLAN IDs for Public Spot users, etc.).

☐ In „Name“ you enter the usernames of future users or the „MAC addresses“ of their end devices.

If you selected the authentication mode „Login with name and password“, enter the name of the username that the user employs to authenticate on the Public Spot. Entering a „password“ is optional, however it is recommended for the authentication mode above.

▶ LANconfig: `RADIUS server:General:User database`



Hinweis: If the authentication is performed using the MAC address (authentication modus „Authenticate with name, password and MAC address“), you define the MAC address using the field „Calling station“ in the format `12:34:56:78:90:AB`.

☐ Set the „Service-Type“ to `Login`.

☐ You remove all protocol restrictions by deselecting all check boxes.

Two-phase authentication is not performed in a Public Spot scenario. This only makes sense for direct WLAN connections without Public Spot operations and the associated RADIUS users.

Hinweis: If you do not completely remove the protocol restrictions, a user cannot log in using the login web page of your Public Spot!

☐ Optional: On request, you can also, for example,

- Enter a relative and/or absolute expiry date for the validity of the user account in the section „Validity/Expiry“ (relative = validity in seconds after the first login);
- Limit the uplink/downlink under „TX“/„RX bandwidth limit“;
- Enable „Multiple login“ and enter the „Max. concurrent logins“ of end devices

☐ Store the configuration on your device.

That's it! Your Public Spot users can now login with the credentials that you specified.

5.4 Security Settings

The Public Spot has two additional safety mechanisms that effectively protect it against abuse.

5.4.1 Traffic Limit Option

In order for clients to login to the Public Spot via a browser, it must be possible for unauthorized users to transfer data packets (e.g. for DNS requests) to the access point. By default, there is no limit on this data. The following risks are associated with this:

- **Unauthorized use of a Public Spot:** Certain tools enable a user to pack data into a DNS packet (i.e. to establish a DNS tunnel) and to work with the Public Spot without logging in.
- **Denial-of-Service:** The attacker could send large amounts of data to the device and thus try to block the device or Public Spot.
- **Brute force:** The attacker could repeatedly try to access the base station by guessing the login data until successfully breaking in.

The traffic limit option can effectively eliminate these risks.

You enable the traffic limit option by setting a value other than "0". This value determines the maximum data quantity in bytes that can be transmitted between the base station and an unauthorized terminal device.

- LANconfig: `Public Spot:Public Spot:Allow access without authentication:Maximum data volume`

When a terminal device exceeds this traffic volume, the Public Spot locks this device and drops all data received from it without inspection. This lock expires only when the device entry disappears from the station table.

Hinweis: For WLAN devices, this deletion can follow the general idle timeout, for example:

- WEBconfig: `HiLCOS Menu Tree:Setup:WLAN:Idle timeout`

Please keep in mind that if station monitoring is active, the lock may be removed earlier. If the mobile station cannot be reached for 60 seconds, the device removes its entry from the station table, and also the block.

Hinweis: The idle timeout for the Public Spot module has the same purpose as the idle timeout for WLANs, but it applies only to connections via Public Spots. If the idle timeout is set and no further data packages are received from a user, the device automatically logs the device out at the end of the specified time period.

- LANconfig: `Public Spot:Public Spot:Idle timeout`

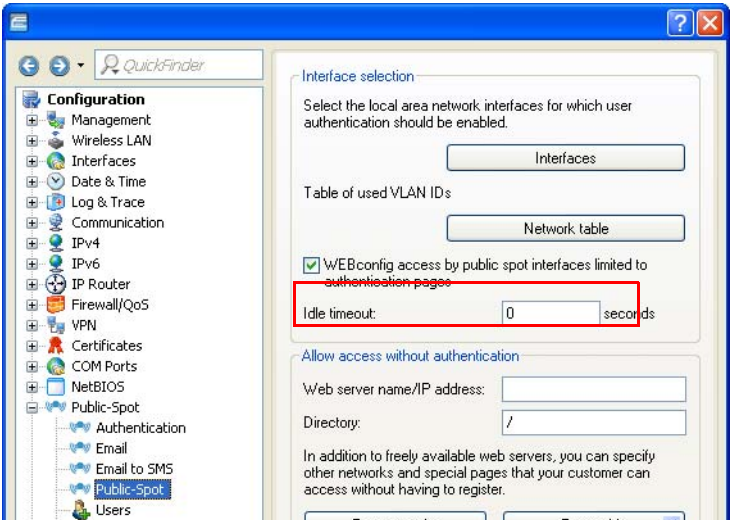
On the one hand the optimal value for traffic limit depends on the data volume of the login page. On the other hand, this value has a significant effect on the potential number of failed login attempts per user. Generally, a traffic limit of 60,000 bytes provides effective protection for a Public Spot but allows a sufficient number of login attempts. You can adjust this value to your individual needs, if necessary. The default value of "0" bytes allows an unlimited volume of data.

Hinweis: The traffic limit option only monitors the traffic before authentication. It does not take into account the traffic to and from a free Web server. This remains unlimited at all times.

5.4.2 Restricting Access to the Configuration

Public Spot access to a Public Spot network's configuration (WEBconfig) should be prohibited for security reasons. A special switch allows access via the Public Spot interface to be restricted to the Public Spot authentication pages only. All other configuration protocols are automatically blocked.

- LANconfig: `Public Spot:Public Spot:WEBconfig access by Public Spot interfaces limited to authentication pages`



Hinweis: Note that you cannot restrict access to the device to HTTP(S) by means of the permissions under `Management:Admin:Configurations access ways:Access rights`.

5.5 Advanced Functions and Settings

The Public Spot offers a wide range of extended functions, options and parameters, which can be used to adapt it to the specific requirements of the application at hand.

In the following sections you will find information about:

- Multiple logins

  By default, the use of login data is restricted to login with one device. Find out how you increase this limit or completely remove this limit for a user account.

- Open access networks (no login)

  Setup additional networks so that Public Spot users can also reach them without logging in to the Public Spot to provide the user with additional information (e.g., customer web sites inside the company, event calendars in a hotel).

- User administration using the Web API

  Use URLs to create and administrate Public Spot users with file links or scripts.

- Automatic cleanup of user accounts and mobile stations

  Use the device's own functions to automatically delete expired Public Spot user accounts and improperly logged off mobile stations (WLAN only) from the device's internal databases.

- WLAN handover of sessions between devices

  Find out more about the roaming possibilities of mobile stations between access points, and what special configurations are necessary so that your users benefit from the seamless handover of WLAN sessions.

- Authentication via RADIUS

  Find out how you can provide multiple RADIUS servers for authentication and accounting, and how you can chain them, in order to forward the user data to the appropriate backup system in case individual systems are unavailable.

- Accounting for Public Spot connections for commercial operation

  Learn more about the accounting functions provided by the Public Spot for commercial operations. These billing functions can be roughly divided into two models:

  - Retrospective payment for the resources actually used (credit accounting)
  - Service use on a debit payment basis (PrePaid)

- Using multi-level certificates

  Find out how to load certificate chains on your device.

- Individual assignment of VLAN IDs

  Find out how to assign individual VLAN IDs to specific Public Spot users.

5.5.1 Multiple Logins

You have the ability to allow Public Spot users to simultaneously sign in using one user account for multiple devices. This can be necessary for a group of people (for example, a family) that has multiple devices, which they would like to use to simultaneously access the Internet. The multiple logins option is enabled for each account individually in the user database of the RADIUS server.

5.5.2 Open Access Networks (No Login)

To provide users with access to important information without them having to login (e.g., important contact information) you can define any publicly available Web server.

- LANconfig: `Public Spot:Public Spot:Web server name/IP Address`

If you do not want to completely release this service, you can optionally define an alternative path to the web server.

- LANconfig: `Public Spot:Public Spot:Directory`

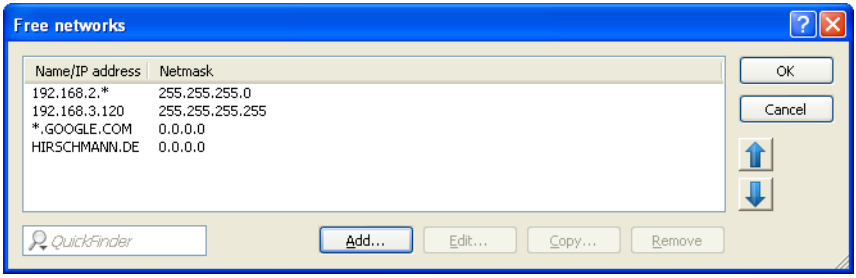
In addition to freely available web servers, you can define other networks and special sites which your customers can access without having to log on.

- LANconfig: `Public Spot:Public Spot:Free networks` or „Page table“

  - „Free networks“

    Enter the IP address of the server or of the network with its netmask, that your Public Spot users are to be given access to. Alternatively, you have the option of entering a domain name (with or without a wildcard "*"). Wildcards can be used, for example, to allow free access to all of the subdomains of a particular domain. The entry `*.google.com` allows the addresses `mail.google.com`, and `maps.google.com`, etc.

    If you wish to authorize a domain or just a single workstation with the address named earlier, set `255.255.255.255` as the netmask here. If you wish to authorize a whole IP network, specify the corresponding netmask. If you do not set a netmask (value `0.0.0.0`), the device ignores the table entry.



  - „Page table“

    Enter the addresses (URLs) of the web pages to be displayed to users on the Public Spot in case of login, error, status display, etc. Also see the chapter about default and customized authentication pages (see page 374).

- DNS Snooping

  Web services with a high number of users distribute the requests for data to multiple servers for better utilization. This means that two DNS queries for the same hostname (e.g. "www.google.com") can lead to two different IP addresses. If a Public Spot receives more than one valid IP address for the specified host name from the DNS server, it chooses one of them and stores it for future requests by Public Spot users. If a different IP address for the same host name is allocated to the user by a different server for a subsequent request, the Public Spot blocks this connection because this IP address is not stored as the authenticated one.

  In order for Public Spot users to be able to connect to the requested host despite changing IP addresses, the Public Spot analyzes the user's DNS queries and stores the returned IP address with the host name, the valid time to live (TTL), the age and the data source as a free destination address in the table `Status:Public Spot:Free-Hosts` for subsequent use.

  The entries in this table will expire after the time period defined in the DNS response (TTL). When the limits are very low (e.g. 5 seconds), you can avoid locking out Public Spot users immediately after a request by setting a minimum validity under `Setup:Public Spot-Module:Free-Hosts-Minimum-TTL`.

5.5.3 Managing Public Spot Users Via the Web API

As an alternative to using the Setup Wizard, entering a special URL in the address bar gives you the option of displaying, creating or deleting Public-Spot users directly.

- URL Structure

  The URL is structured as follows:

  ```
  http://<Device-URL>/cmdpbspotuser/
  ?action=actiontodo&parameter1=value1&parameter2=value2
  ```

The following actions are available:

- **action=addpbspotuser**: Creates one or more new Public Spot users and then prints out the required number of vouchers.
- **action=delpbspotuser**: Deletes the Public Spot user with the specified user ID.
- **action=editpbspotuser**: Displays the Public Spot user with the specified user ID. You can then print out the user's voucher again.

The required parameters and their values depend on the action specified.

Hinweis: The Wizard ignores incorrect parameter information and accepts only the correct parameters. If you omit a required parameter or specify it incorrectly, the wizard displays an input mask. Enter the correct parameter values here.

Adding a Public Spot User

To register a new Public Spot user, simply enter the following URL:

```
http://<Device-URL>/cmdpbspotuser/
?action=addpbspotuser&parameter1=value1&parameter2=value2&...
```

The following parameters are available to you:

☐ `comment`

Comment on the registered user

If it is possible to enter multiple comments for a Public Spot user, you can enter the comments and their corresponding comment-field names as follows:

☐ `&comment=<Content1>:<FieldName1>,<Content2>:<FieldName2>,...,<Content5>:<FeildName5>,`

If there is only one comment field for each user, it is sufficient to enter the comment:

☐ `&comment=<Comment>`

Hinweis: Special characters such as German umlauts are not supported.

Hinweis: The maximum number of characters for the comment parameter is 191 characters.

☐ `print`

Automatic print-out of the voucher.

If this parameter is omitted, the wizard displays a button that you can use to print the voucher.

☐ `printcomment`

Print the comment on the voucher.

If this parameter is omitted, no comment will appear on the voucher (default setting).

☐ `nbGuests`

Number of Public Spot users to be created.

If this parameter is omitted, the wizard creates one user only (default setting).

☐ `defaults`

Use default values

The wizard replaces missing or incorrect parameters with default values.

☐ `expirytype`

Combined output of expiry type and validity period of the voucher.

Enter this parameter as follows:

☐ `&expirytype=<value1>+validper=<value2>`

The parameter values have the following meanings:

- `Value1`: Expiry type: Possible values are `absolute`, `relative`, `both` and `none`.
- `Value2`: Validity period of the voucher if `expirytype` has the value `both`. In this case, you use `validper` to specify the maximum validity period of the voucher in days for the absolute expiry. For all other expiry types, the parameter `validper` is not set.

If a parameter is missing, or if you enter incorrect values, the wizard uses the default values.

☐ `unit`

Access time

Specify this parameter as follows:

☐ `&unit=<Value1>+runtime=<Value2>`

The parameter values have the following meanings:

- `Value1`: LIfetime units. Possible values are: Minute, hour, day
- `Value2`: Duration

☐ `timebudget`

Time budget

If this parameter is omitted, the wizard uses the default value.

☐ `volumebudget`

Volume budget

If this parameter is omitted, the wizard uses the default value.

Hinweis: If the Public Spot administration contains no default values to replace missing parameters, the wizard opens a dialog. Enter the missing values here.

Modifying a Public Spot User

Modify one or more Public Spot users simply by entering the following URL:

```
http://<device-URL>/cmdpbspotuser/
?action=editpbspotuser&parameter1=value1&parameter2=value2&...
```

The following parameters are available to you:

☐ `pbspotuser`

Name of the Public Spot user

Specify multiple users in the form `&=pbspotuser=<User1>+<User2>+....`

If the wizard cannot find the specified user, you have the option to search for a user.

After making your changes, accept these and print them out if necessary.

☐ `expirytype`

Combined output of expiry type and validity period of the voucher.

Enter this parameter as follows:

☐ `&expirytype=<value1>+validper=<value2>`

The parameter values have the following meanings:

- `Value1`: Expiry type: Possible values are `absolute`, `relative`, `both` and `none`.
- `Value2`: Validity period of the voucher if `expirytype` has the value `both`. In this case, you use `validper` to specify the maximum validity period of the voucher in days for the absolute expiry. For all other expiry types, the parameter `validper` is not set.

If a parameter is missing, or if you enter incorrect values, the wizard uses the default values.

☐ `unit`

Access time

Specify this parameter as follows:

☐ `&unit=<Value1>+runtime=<Value2>`

The parameter values have the following meanings:

- `Value1`: LIfetime units. Possible values are

  Minute

  Hour

  Day

- `Value2`: Duration period

☐ `timebudget`

Time budget

If this parameter is omitted, the wizard uses the default value.

☐ `volumebudget`

Volume budget

If this parameter is omitted, the wizard uses the default value.

☐ `print`

Automatic print-out of the voucher.

If this parameter is omitted, the wizard displays a button. Use this to print out the voucher.

Hinweis: If the Public Spot administration contains no default values to replace missing parameters, the wizard opens a dialog. Enter the missing values here.

Deleting a Public Spot User

Delete one or more Public Spot users simply by entering the following URL:

```
http://<deviceURL>/cmdpbspotuser/
?action=delpbspotuser&pbSpotuser=<User1>+<User2>+...
```

If the wizard finds the specified user in the user list, it deletes the user and outputs a corresponding message.

If the wizard cannot find the specified user, it displays a table of registered Public Spot users. Mark the entries for deletion here.

5.5.4 Clear User List Automatically

The device gives you the option to delete expired accounts for Public Spot users automatically.

Users of the Public Spot Wizard are generally administrators with restricted rights who are often unable to delete user table entries themselves. Because the user table has a limited number of entries, outdated entries could limit the capacity of the Public Spot. We strongly recommend that you activate this option.

If you use the internal RADIUS server for the administration of user accounts, enable automatic clean-up under `RADIUS server:General:Clear user lists automatically`.

Hinweis: These settings have no effect on the user table on an external RADIUS server.

5.5.5 Station Monitoring

If station monitoring is activated, the Public Spot regularly checks to see if the associated end devices are still available. Lost end devices are automatically deleted from the local user table. If station monitoring is switched off, a user is not logged off until the validity period of the user's authentication expires.

Hinweis: Station monitoring is extremely important for Public Spots operating commercially on a time basis. In installations of this type, users must be assured that they are only paying for the time actually spent using the Public Spot services.

- Configuration

  Hinweis: If your device has WLAN, you also have the option of enabling station monitoring globally for all WLAN interfaces. You can find the corresponding settings under `Wireless LAN:Security:Monitor stations` to detect inactive ones. To do this, the device disconnects mobile stations after 60 seconds (default value). If WLAN station monitoring is disabled, this may take up to an hour.

If you offer Public Spot via WLAN, please note that the station monitoring of the WLAN takes priority over that for the Public Spot, and a disconnection can occur earlier if the idle timeout for WLAN (configurable in the Setup menu under `WLAN:Idle timeout`) is less than that for the Public Spot.

Station monitoring for the Public Spot Module is disabled by default. You activate it by entering a value greater than `0` under `Public Spot:Public Spot:Interface selection:Idle timeout`. This value disables the function. From this point on, all end devices are automatically disconnected from the Public Spot after a specific time.

Monitoring

You can monitor the Public Spot during operation using WEBconfig. The station table in the user authentication menu provides an overview of:

- Users currently logged in to the Public Spot and
- End devices in the WLAN which are not logged in.

You can navigate to the Station table in the Status menu under `Public Spot:Station Table`. Using the button „Monitor this table“ you automatically refresh the table display at regular intervals.

5.5.6 WLAN Handover of Sessions Between Devices

Whenever a site equipped with WLAN hotspots expands, it may be necessary to deploy more than one access point to cover the whole area. One option would be to use a central device as an authentication gateway, enable the Public Spot option on this device only, and require all other access points to redirect requests to the central device. In this way, all other access points act as simple, transparent bridges, which connect to the central gateway using the Ethernet backbone. This allows clients to freely roam among the access points since all session information is kept in the central gateway.

This variant has two drawbacks, however:

- The central gateway is a single point of failure, and is not scalable. You can reduce the risk of failures by using VRRP to create a redundancy solution.

  Hinweis: This solution requires an external RADIUS server, since VRRP cannot synchronize configurations, e.g. the user database. However, this means that certain functions (such as the Public Spot wizards in WEBconfig) are no longer available.

- Roaming is only necessary when the Public Spot module is installed on the access points themselves. Using a WLC, the authentication can be forwarded to the central gateway. In this case, the roaming between access points is transparent to the WLAN controller.

An alternative to this type of centralized setup is to enable the Public Spot module in all of the access points. Authentication and page processing handling is thereby distributed over all devices, and a single point of failure is eliminated.

IAPP (Inter Access Point Protocol)

Since the Public Spot module is implemented as a "switchable" transparent bridge, there is no need for clients to acquire a new IP address after they roamed to another access point, so there is no need to terminate open connections. This results in the requirement that an already authenticated client does not have to re-authenticate after roaming to a new access point. Thus the authentication information should be carried over from the old to the new access point.

Access points use the IAPP (inter access point protocol) to share information about roaming clients: Whenever a wireless client decides to change to another access point, it has the option of informing the new AP about which AP it was previously connected to. This information, combined with regular Hello packets on the Ethernet backbone, enable the new access point to inform the old access point. The old access point can then remove the client from its station table and acknowledge the handover.

If a client does not use the corresponding Reassociate packet for connecting to the new access point, the new access point sends a handover request as a multicast on the backbone, instead of a directed packet to the old access point. This means that this handover also works for clients that do not support IAPP.

The main task of the IAPP in a WLAN is to tell the old access point not to send any more packets to the corresponding client in its wireless area, since it will no longer receive them. This type of behavior (based on the definition of the 802.11 frame exchange protocol) could otherwise cause problems with other clients that are connected with it.

In case of an enabled Public Spot module, the communication channel provided by IAPP is used to transport the session information of wireless clients. Whenever an access point receives a handover request for one of its wireless clients, and if a session record for this client is available in its station table, it will append state information about this client to the requesting access point. This information includes:

- The client?s current state (authenticated or not authenticated).

  In case the client is authenticated, it also includes:

  – The username used to authenticate
  – The amount of data traffic generated by the client so far
  – The session duration so far
  – The IP address of the client
  – Possible limits on the session duration and data volumes
  – Possible information about idle timeouts

- If RADIUS accounting was used for the session:

  – The entry used for RADIUS accounting in the authentication server list, referenced by name
  – The accounting cycle used for interim updates

After a successful transfer, the old access point terminates the session, which, in the case of RADIUS accounting, means that it sends an accounting stop request to the RADIUS accounting server. This is necessary since a RADIUS server can use the NAS identification to associate requests with specific sessions, and these requests can no longer be associated with the correct sessions once the data packets for a session come from more than one device. If an access point receives this information in a handover reply, it immediately marks the client as authenticated and starts a new RADIUS accounting session, if possible.

Hinweis: Note that the new access point requires a corresponding entry in its „Authentication server“ list in order to receive the necessary information. The specific part of the handover reply for the Public Spot module is protected by a shared secret, which is set in the setup menu under `Public-Spot-Module:Roaming-Secret`. These security measures should prevent falsification of handover replies. Without a password configured, the access point does not append the information above on a handover reply, which forces the client to authenticate again.

5.5.7 Authentication via RADIUS

RADIUS is an extensively accepted protocol for providing large groups of users access to a server. Although it was originally developed for dial-in server access over telephone lines, the concept is also useful for the hotspot authentication process. For that reason, it can be used in a more complex provider network, for example, to provide access for the same users via dial-in and hotspots. You configure RADIUS servers and their access parameters in the dialog `Public Spot:Public Spot` under „Authentication servers“.

In certain scenarios, it can be feasible to use more than one RADIUS server. In general, a RADIUS server is specified by its IP address, the UDP port the RADIUS service is bound to (typical ports are 1645 or 1812), and a so-called "shared secret". This is a random character string which acts as a password for access to the server. Only clients which know the shared secret can interact with the RADIUS server, since the password for the user account is hashed instead of being sent in plain text.

In theory, the simplest possible RADIUS transaction consists of the device sending the entered account data (user name + password) to the RADIUS server and the RADIUS server responding with either "yes" or "no". However, the RADIUS protocol also allows more complex responses and requests where the communication partners use a list of variables ? so-called "attributes" ? for requests and responses. Starting from page 392 you will find a list of which attributes a device can send to a RADIUS server and which attributes from a RADIUS response are understood by the device.

Multiple Authentication Servers

As mentioned previously, the list of authentication servers can contain more than one entry. There may be situations where the hotspot provides access to the Internet for customers from different service providers. These providers may have separate user databases and their own RADIUS servers. The device must select which provider corresponds to the user based on the username.

Whenever the device does not find an entry for an authenticated user in its local table, it will first search through the authentication server list to find the provider that corresponds to the user. For example, user account names like `JohnDoe@hirschmann.de` contains the authentication server entry named `HIRSCHMANN`. If the first allocation does not work, the device attempts to allocate the entry `DEFAULT` to the user. If this entry also does not exist, the device selects the authentication server that is first in the list. If the device does not find an entry (i.e., the list is empty), the user authentication fails.

Depending on the allocation of a user to a authentication server, your device always transmits the complete username to the selected RADIUS server. The selected RADIUS server is stored as the provider for the subsequent session and used for optional RADIUS accounting.

Chaining of Backup Servers

Internet access providers wish to provide a very high level of availability, and a common method to achieve this relies on redundancy. This redundancy is achieved using the backup servers which are needed when a request times out on the primary server, for example, because the server or another network component along the way was unavailable.

The requirements for backup servers varies widely among the different providers, which is why the list of authentication servers does not have a specific number of input fields. Instead, the device offers you a series of backup servers (backup chaining). Here, two or more entries in the authentication server table may be chained together to form a list of RADIUS servers. The device looks through the list of RADIUS servers one by one until the end of the list is reached (authentication failure due to server unavailability) or a response from a server (either positive or negative) is obtained.

You chain backup servers using the input field „Backup name“ in the add/edit dialog under `Public Spot:Public Spot:Authentication server`. Whenever a RADIUS request fails (i.e. times out), the device checks the backup field, and continues to try the RADIUS server specified in the entry that is referenced by the backup name. In general, an unlimited number of servers can be connected this way, which makes it possible for several providers to assign the same fallback server. The chain of backup servers is considered to be terminated if one of the following conditions occurs:

- Querying a RADIUS server failed and the corresponding authentication server table entry has an empty backup field.
- Querying a RADIUS server failed and the corresponding provider table entry has an invalid backup field, i.e. the entry referenced is not present in the authentication server list.
- Querying a RADIUS server failed and the corresponding authentication server list entry refers to an entry that has already been used in the query process. This avoids endless RADIUS requests due to circular references. It is possible to specify two RADIUS servers that reference each other as backups, with the primary server being selected by the user account name.

Hinweis: While the device is sending a RADIUS request, the TCP/HTTP connection to the client still exists. If the runtime of the chaining exceeds the lifetime of the TCP/HTTP connection, the client interrupts the login attempt. Therefore, it may be recommended to reduce the number of request retries to the individual backup servers as well as the time intervals between requests. These settings can be made in `RADIUS server:Options`.

5.5.8 Billing Without a RADIUS Accounting Server

If user administration is performed using the internal user list of the Public Spot module, and you do not want to use a RADIUS accounting server, your only option is to use the expiry date of the user account for accounting purposes.

The use of the internal user list is no longer recommended. Instead, in order to take advantage of all of the options the Public Spot offers, you should use the internal RADIUS server for new installations.

Hinweis: For the purposes of billing by credit payment, the Public Spot can use SYSLOG to output detailed connection information to any computer in the network. Using the appropriate software on the destination computer allows you to precisely bill the resources that were actually used (such as connection times or transfer volumes).

5.5.9 Billing via RADIUS Accounting Server

For the purposes of billing via a RADIUS server, you can set up the Public Spot so that it regularly supplies the current connection information for every active user to the specified accounting server. Accounting is started when a client is authenticated using RADIUS and a valid „Accounting server“ is configured for the relevant „Authentication server“ in the list of „Authentication servers“. It is possible to use different RADIUS servers for authentication and accounting.

Each of the regular message packets to the accounting server contains information about the resources (time, transferred data volumes, etc.) consumed by the user since the last message. This means that, even in the worst case of a Public Spot failure (e.g., due to a power outage or similar), only a small amount of accounting information will be lost.

Periodic messaging of accounting information to the accounting server (interim updates) is deactivated by default. It is activated by setting a value for the accounting cycle which is greater than 0.

- LANconfig: `Public Spot:Users:Update cycle`

Hinweis: This cycle is defined in seconds. This sets the time interval of when your device regularly sends connection information to the accounting server. Setting the cycle to `0` deactivates this function. If this is the case, your device only sends accounting information at the beginning and end of the session.

When accounting on a prepaid basis, the RADIUS server monitors the restrictions on the users (limits on connection times or transfer volumes, expiry date). As soon as a user has used up the prepaid amount, the RADIUS server locks the user account. Your device rejects future login attempts for the user.

Hinweis: Time limits for prepaid models can be monitored by the Public Spot during active sessions. If a time limit is exceeded, the Public Spot automatically terminates the corresponding session. The monitoring of prepaid amounts is possible if the RADIUS server transmits the user's time credit to the Public Spot as the "Session timeout" attribute at the start of the session.

Request Types

Your device is able to send different types of RADIUS requests to an accounting server. These requests differ according to a user's session state:

- An accounting start request is sent after a successful authentication.
- An accounting stop request is sent after a Public Spot session is terminated.
- Optional: Interim updates are sent throughout the session.

There are two types of interim updates: An initial update is sent immediately after the start request since some RADIUS servers need this in order to create a session in the accounting database. All further updates depend on whether an accounting cycle was created for the respective session (see `Public Spot:Users:Accounting update cycle`).

Alternatively, this value may be included in a RADIUS authentication response: The RADIUS server offers the RADIUS client (for example, your Public Spot) an interim accounting interval, which the client will use if it has the appropriate support for this and as long as no interval was set locally on the device itself.

Hinweis: If a local value was set, it will always be given a higher priority than the one received from a RADIUS server, which the RADIUS RFCs require by default!

Starting from page 392 „Commonly Transmitted RADIUS Attributes“ you will find a list of which attributes a device can send to a RADIUS server and which attributes from a RADIUS response are understood by the device.

Accounting Backup

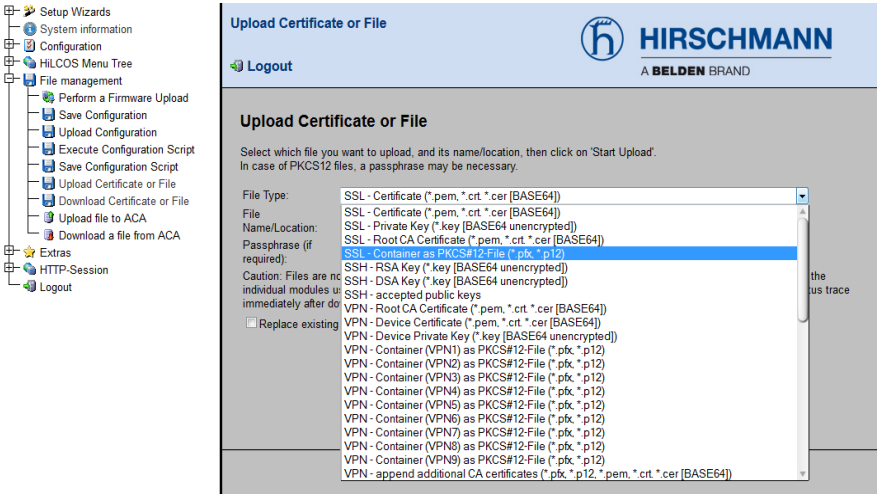
The backup solution for RADIUS accounting is the same as the one for RADIUS authentication, in that your device goes through the entries in the authentication server list one by one (see page 350 „Chaining of Backup Servers“). The backup entries for the accounting server should be chosen with the same care as for the authentication server: If you are using multiple backups, you will probably have to reduce the timeout/try values for the requests in order to achieve reasonable response times for the entire system.

Hinweis: User sessions are not paused while the device sends accounting requests, which consumes additional resources in the device?in contrast to authentication. Please ensure that the time required for the selection of an accounting server* should be less than the length of an accounting cycle for interim update requests. This stops the requests from queuing up, which would result in a stack overflow.
*** Number of backups x (idle timeout + number of retries)**

5.5.10 Multilevel Certificates for Public Spots

SSL certificate chains can be loaded into the device as a PKCS#12 container. These certificate chains can be used for Public Spot authentication pages by using the HTTPS server implemented in the device. Certificates from recognized trust centers are normally multi-level. Officially signed certificates in the Public Spot are necessary to avoid certificate-related error messages from the browser when authenticating at a Public Spot.

The certificate is loaded into the device for example by using WEBconfig in File Management to upload the individual files of the root CA certificate or a PKCS#12 container:



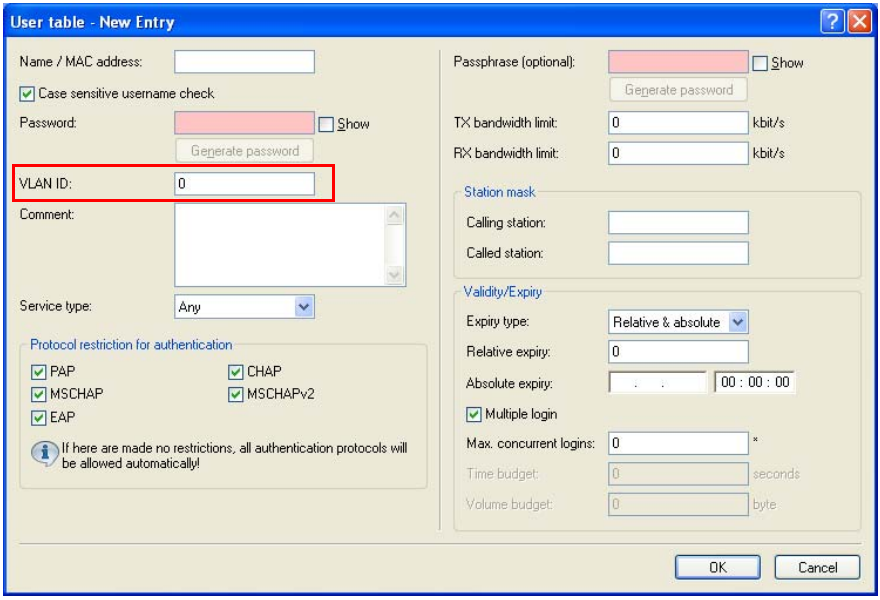
Certificates are normally issued for DNS names, so the Public Spot must specify the certificate's DNS name as the destination and not an internal IP address (enter in `Setup:Public Spot Module:Device Host Name`). This name has to be resolved by the DNS server to provide the corresponding IP address of the Public Spot.

5.5.11 Assigning Users to Individual VLANs

Regardless of the assignment of a VLAN ID for the entire Public Spot module, the device offers you the option of separately assigning individual VLAN IDs for individual Public Spot users. This ID is automatically assigned by the RADIUS server to your users after successful authentication. In this way it is possible, for example, to classify different Public Spot users in

separate networks with different access rights and access options without having them login to separate SSIDs or requiring you to publicize the availability of various networks (e.g., networks for different customer types). The relevant rules can be realized via the firewall by specifying the VLAN ID of the respective user/the relevant user groups as the source tag.

Hinweis: An enabled VLAN module is a prerequisite for the functions described above.



- Open the „User table“ in the dialog „RADIUS server “„General“ and click „Add...“ to create a new user.
- Assign an individual VLAN ID to the new user with the input field „VLAN-ID“. After authentication by the RADIUS server, the individual VLAN ID overwrites a global VLAN ID that a user would otherwise obtain from the interface. The value `0` disables the assignment of an individual VLAN ID.

Hinweis: For technical reasons, the assignment of a VLAN ID requires a new address assignment by the DHCP server. As long as a client is not yet assigned a new address after successful authentication, the client is still in the previous (e.g., untagged) network. In order for the clients to be transferred to the new network as quickly as possible, it is necessary to set the lease time of the DHCP server as low as possible under `IPv4:DHCPv4`. Possible values (in minutes) include, for example:

- „Maximum lease time:“`2`
- „Default lease time:“`1`

Take into account that a strong reduction in global lease time can flood your network with DHCP messages, and when there is a larger number of users, it leads to an increased network load! Alternatively, you have the option of using an external DHCP server or allowing your users to manually request a new address by using their client. In the Windows command line this is done, for example, using the commands `ipconfig /release` and `ipconfig /renew`.

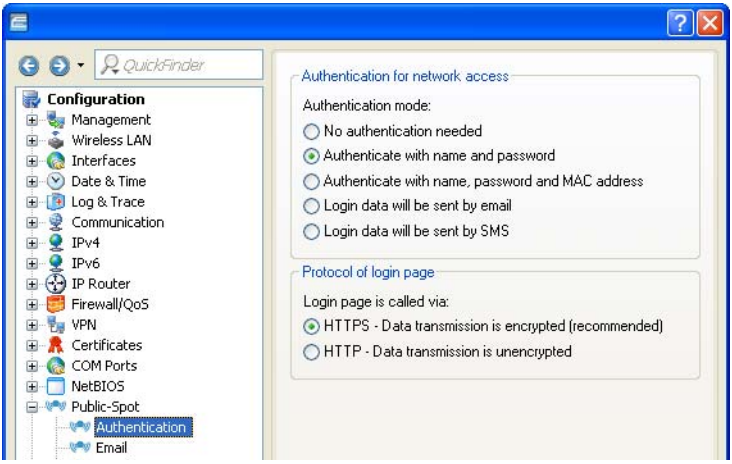
Hinweis: By assigning a VLAN-ID, the user loses his connection after the initial DHCP lease expires. The connection only remains stable as of the second lease, i.e. after successfully assigning the VLAN-ID.

5.6 Alternative Login Methods

In addition to the login using the login data that was sent previously, your users can also request login data themselves via e-mail or text message (SMS). Alternatively, you can link your Public Spot to other software systems using the XML interface in order to implement more complex or multi-level login scenarios.

5.6.1 Overview of Authentication Modes

The settings for network authentication are to be found in the LANconfig dialog `Public Spot:Authentication`.



The following authentication modes are available:

- „No authentication required“

  Users get free access to the Public Spot, authentication is not required.

  Hinweis: Do not use this setting if your device has unlimited access to the Internet.

- „Authenticate with name and password“

  Users log on to the Public Spot with their name and their password. Users get their login data from a network administrator as a voucher.

- „Authenticate with name, password and MAC address“

  Users log on to the Public Spot with their name and their password. Users get their login data from a network administrator as a voucher. For this login mode, the MAC address of the client must also match the one stored in the user list by the administrator.

- „Login data will be sent by e-mail“

Users log on to the Public Spot with their name and their password. Users generate the credentials themselves, and the data is sent via e-mail. No action by an administrator is necessary.

- „Login data will be sent by SMS (text message)“

  Users log on to the Public Spot with their name and their password. Users generate the credentials themselves, and the data is sent by SMS (text message). No action by an administrator is necessary.

5.6.2 Independent User Authentication (Smart Ticket)

Devices operating a Public Spot provide users with time-limited access to wireless networks. Until now an administrator account was necessary to create a login on a device with the Public Spot. For employees at a hotel reception desk, for example, you can set up an administrator account that only has the function rights to create Public Spot users. With a few mouse clicks the employee can print a voucher for the hotel guests for access to the wireless network.

However, the easy voucher solution still requires action from an administrator. Alternatively, you can give the users the option to generate their own login data for the wireless network from the homepage of the Public Spot, and send it to themselves by e-mail or SMS (text message). In order to send e-mail, an SMTP account must be fully set up in the device settings. To send SMS/text messages the device uses an external SMS provider, which can charge fees to the Public-Spot operator or user, if desired.

The settings for sending login credentials by e-mail are to be found in the LANconfig dialog `Public-Spot:E-mail`. Those for sending via SMS are in the dialog `Public Spot: E-mail to SMS`.

5.6.3 Automatic Authentication with the MAC Address

After successful authentication, a Public Spot gives the user access to certain services. The Public Spot usually displays a login website to allow users to authenticate themselves. The user enters the authorization credentials into the login page and the Public Spot then redirects the user to the allowed sites.

In some applications, authentication via web site may not be desired or not possible, as the following examples illustrate:

- The end device does not have a browser and therefore cannot open the login page.
- Manually accessing the login page may be undesirable, such as when carrying out a performance test.

Automatic authentication on the Public Spot with a MAC address makes it possible to use the Public Spot without first opening the login page. The administrator enters the MAC addresses of the corresponding end device into the table of permissible MAC addresses under `Public Spot:Users:MAC authenticated users`.

The MAC-address Check Procedure

When the device receives a request from a client, the Public Spot executes the following steps for the automatic authentication by MAC address:

- If the Public Spot has already authenticated the MAC address of the received data packets, the device forwards the data packets without further delay.
- If the MAC address is in the list of allowed clients, the Public Spot starts a new session for the user and forwards the corresponding data packets.
- If a provider has been defined for verification of the MAC addresses by RADIUS, and a positive, valid MAC address authentication is cached in the Public Spot, then the Public Spot starts a new session for that user and forwards the associated data packets.
- If a provider chooses to check the MAC address with the RADIUS server, but does not have a valid authentication for the MAC address saved in the cache of the Public Spot, the Public Spot starts authentication on the corresponding RADIUS server. After a positive response, the Public Spot starts a new session for that user and forwards the associated packets.
- All of the above checks are unsuccessful, the Public Spot directs the user to the login page.

Authentication of the MAC Address by RADIUS

If the MAC address of a WLAN client requesting to associate is not included in the list of permissible addresses, the Public Spot can alternatively authenticate the address via a RADIUS server.

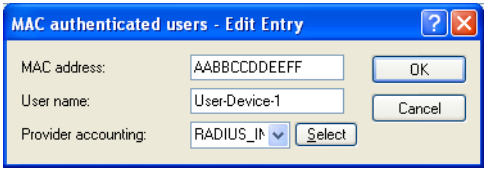
To enable RADIUS authentication, the administrator selects one of the RADIUS servers that has defined in the device and saved to the list of providers.

In addition, the administrator defines a lifetime for the rejected MAC addresses. This lifetime is used by the Public Spot to prevent the RADIUS server from being flooded with repeated requests for MAC addresses which cannot be authenticated (without login) via the RADIUS server or MAC address table.

If a MAC address authentication is rejected by the RADIUS server, the Public Spot saves this rejection for the lifetime defined here. Further requests for the same MAC address within the lifetime are answered directly by the Public Spot, without forwarding them to the RADIUS server first.

Configuration in LANconfig

For the configuration in LANconfig, you can find the parameters for authenticating clients by means of their MAC address in the dialog `Public Spot:Users:MAC authenticated users`.



5.7 XML Interface

In order to be able to cover a wide range of Public Spot scenarios, the default authentication method of name and password is not sufficient by itself. Access and accounting models using key cards, dongles or prepaid credit cards often require additional access data, which the Public Spot in this form would be unable to manage.

The implemented XML interface connects the Public Spot and an external gateway. It directs the user data only to the gateway that handles the authentication and accounting, and it only sends information about the duration and limits of the user access to the Public Spot.

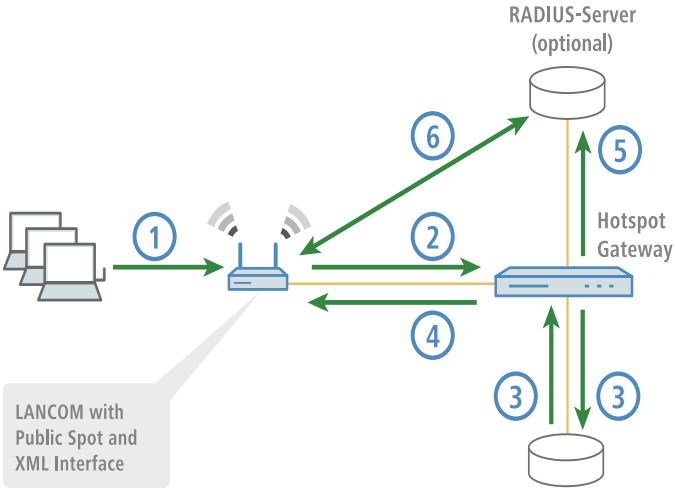
In this case, the Public Spot only performs the following tasks:

- Forward the user requests
- Restrict unauthorized access attempts
- Accept gateway commands to start and stop a session
- Accounting for sessions, if applicable

Since it is not realistic to implement all existing, and at times very specific scenarios with the associated gateway commands on the Public Spot, the XML interface was designed to be flexible and multi-purpose.

5.7.1 Function

The communication between the XML interface and external gateway is processed as follows:



☐ The user connects to the Public Spot's WLAN and sends an HTTP request to the Public Spot.

☐ The Public Spot forwards the login procedure's HTTP request to the external hotspot gateway. The external hotspot gateway is located either in a freely accessible network provided by the Public Spot, or its address is included in the list of free hosts.

The Public Spot forwards the MAC address of the requesting Public Spot client to the external gateway. To implement this, navigate to `Public-Spot-Module:Page-Table`, set the „Type“ to "Redirect" and suffix the „URL“ with the parameter `?myvar=%m`.

Example:?`http://192.168.1.1/?myvar=%m`

In this case, `myvar` is a freely selectable variable. The variable `%m` is vital here, as the Public Spot replaces this with the client's MAC address when forwarding the request.

☐ The hotspot gateway checks the user's credentials and, if applicable, it can contact further systems to charging to credit card, for example.

☐ The hotspot gateway sends an XML file with the user data to the Public Spot's XML interface. The external hotspot gateway contacts the device with the Public Spot XML interface using the URL `http://<Device-URL>/xmlauth`.

The Public Spot's XML interface analyses this file and initiates the corresponding actions. In the case of a login request, the XML interface inserts the user and the corresponding MAC address into the list of logged-on Public Spot users. In the case of a logout request, the XML interface removes the user from this list again. At the same time, the XML interface confirms the request by sending a corresponding XML file to the hotspot gateway.

In order for the Public Spot to be able to process the instructions in the XML file, a special administrator must be set up on the device who has the function right "Public-Spot -XML-interface". This hotspot gateway logs in to the Public Spot with this admin account.

While the user is logged in to the Public Spot, the XML interface and hotspot gateway can exchange status information about the current session in the form of XML files.

If the user has exhausted his online quota, the hotspot gateway will send a stop command to the XML interface, and then the Public Spot locks further access for that user. The XML interface also confirms that the login is blocked by sending the corresponding XML file to the hotspot gateway.

☐ If the additional use of a RADIUS server is enabled, the hotspot gateway optionally creates a user in a RADIUS server.

☐ The Public Spot sends relevant data to the RADIUS server throughout the session, for example to facilitate the accounting of the Public Spot usage. By default, the Public Spot uses its internal RADIUS server for this. If necessary, you can configure the device running the Public Spot to conduct forwarding to an external RADIUS server.

Hinweis: Communications between the Public Spot and a hotspot gateway with the use of XML is not standardized. Configure the hotspot gateway according to the instructions in the chapter 367 „Commands“ in order for the Public Spot and hotspot gateway to exchange the XML messages in the required form. XML messages are exchanged invisibly without a graphical user interface. You can use tools such as cURL to test the exchange of messages (see page367 „Commands“).

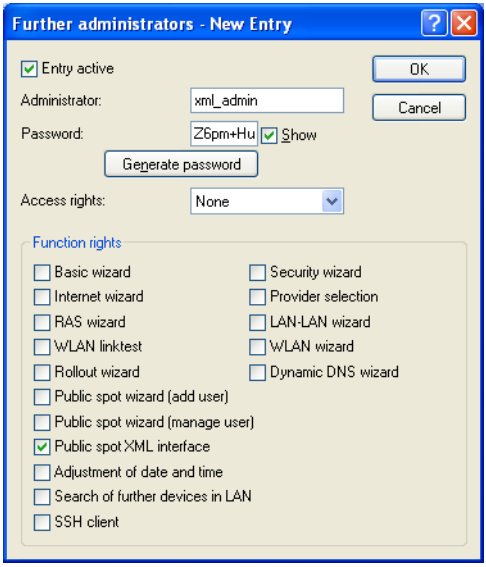
5.7.2 Setting up the XML Interface

The following section describes how to set up the XML interface.

Hinweis: You need to have the "Supervisor" permission in order to create another administrator account.

☐ Using `Management:Admin:Further administrators` you create a new administrator with the function right „Public Spot XML interface“.

This is the administrator account that the gateway uses to send XML files to the Public Spot XML interface.



Hinweis: The new administrator should not have any further Public Spot function rights, since they represent a potential security risk in combination with the XML interface (e.g., if the communication between XML sender and device is unencrypted).

☐ You enable the XML interface in `Public Spot:Public Spot` in the section „External hotspot gateway“ and, if necessary, global RADIUS authentication for your Public Spot.

☐ In the section „Allow access without authentication“ click on the button „Free Networks“ and add a new network. Enter the „Name/IP address“ of the login page. In „Netmask“ enter `255.255.255.255`.

When defined as a free network, the user has direct access to the login page of the gateway without having to login to the Public Spot first.

☐ Configure the gateway so that it sends the user's session data to the Public Spot XML interface as an XML file.

For questions about configuring the gateway, please refer to the applicable service provider.

5.7.3 Analyzing the XML Interface with cURL

The following section describes the analysis of the XML interface with the open-source software cURL.

Client for URL, or cURL, is a command line application use for transferring files on a network without the use of a Web browser or FTP client. "cURL" is a component of many Linux distributions and is also available for other operating systems.

Hinweis: To analyze the XML interface using cURL, you need an administrator account with the function right "Public Spot XML interface" for the Public Spot.

☐ First download cURL and install or unpack it.

☐ Start cURL with the console command

```
curl -X POST -H "Content-Type:text/xml" -d @filename
http://user:pass@myhost/xmlauth/
```

The parameters have the following meaning:

- **@filename**

  Path and name of the local XML file, e.g. the login request from the examples (see page 367 „Login“).

- **user**

  Username with the function right titled "Public Spot XML interface". The XML feature does not work without this authentication.

- **pass**

  User password

- **myhost**

  IP address or DNS name of the OpenBAT device with the Public Spot XML interface

☐ With Telnet you can use the command `trace # XML-Interface-PbSpot` to activate a trace that verifies whether XML requests were successful or error messages were received.

5.7.4 Commands

The XML interface can process three types of requests and responses:

- Login
- Logout
- Status

An XML file can contain several requests and responses.

Login

If the external gateway sends a "Login" request in an XML file, the Public Spot activates online access for the corresponding user. A "Login" request contains the attribute `COMMAND="RADIUS_LOGIN"`.

If the Public Spot does not use a RADIUS server, a "login" request prompts it to store the user and the associated MAC address directly in the internal Status table. As a result, the user is immediately authenticated in future, and there is no need to display a login page for entering the username and password. When you operate a RADIUS server, a 'login' request can only be successfully processed if the login data of the corresponding user already exists on the RADIUS server.

Hinweis: The Web API in the Public Spot provides you with a convenient tool for creating new Public Spot users on the device's internal RADIUS server.

The XML interface can process the following XML elements for a request:

☐ `SUB_USER_NAME`

User name

☐ `SUB_PASSWORD`

User password

☐ `SUB_MAC_ADDR`

MAC address of the user's device Possible formats include:

- 00164115208c
- 00:16:41:15:20:8c
- 00-16-41-15-20-8c

The XML interface then sends the gateway a "Login" response, which can contain the following XML elements:

☐ `SUB_USER_NAME`

User name

☐ `SUB_STATUS`

The current user status. The following values are possible:

- RADIUS_LOGIN_ACCEPT:?Login successful
- RADIUS_LOGIN_REJECT:?Login rejected

☐ SUB_MAC_ADDR

MAC address of the user's device Possible formats include:

- 00164115208c
- 00:16:41:15:20:8c
- 00-16-41-15-20-8c

Some examples of XML files are given below:

☐ **Login-Request**

The external gateway sends the data for the start of a session to the Public Spot:

☐
```
<?xml version="1.0" encoding="ISO-8859-1"?>
<PUBLICSPOTXMLINTERFACE>
??<ACCESS_CUBE COMMAND="RADIUS_LOGIN">
????<SUB_USER_NAME>user2350</SUB_USER_NAME>
????<SUB_PASSWORD>5juchb</SUB_PASSWORD>
????<SUB_MAC_ADDR>00164115208c</SUB_MAC_ADDR>
??</ACCESS_CUBE>
</PUBLICSPOTXMLINTERFACE>
```

The Public Spot enables 'user2350' in the internal Status table.

☐ **Login-Response:**

The XML interface sends a confirmation about the start of a session to the external gateway:

☐
```
<?xml version="1.0" encoding="ISO-8859-1" ?>
<PUBLICSPOTXMLINTERFACE>
??<ACCESS_CUBE ID="WLC-4006_PM" IP="192.168.100.2"
COMMAND="USER_STATUS">
????<SUB_STATUS>RADIUS_LOGIN_ACCEPT</SUB_STATUS>
????<SUB_MAC_ADDR>00:16:41:15:20:8b</SUB_MAC_ADDR>
????<SUB_USER_NAME>user2350</SUB_USER_NAME>
????<TXRATELIMIT>0</TXRATELIMIT>
????<RXRATELIMIT>0</RXRATELIMIT>
????<SECONDSEXPIRE>0</SECONDSEXPIRE>
```

```
????<TRAFFICEXPIRE>0</TRAFFICEXPIRE>
????<ACCOUNTCYCLE>0</ACCOUNTCYCLE>
????<IDLETIMEOUT>0</IDLETIMEOUT>
??</ACCESS_CUBE>
</PUBLICSPOTXMLINTERFACE>
```

Logout

If the external gateway sends a "Logout" request in an XML file, the Public Spot blocks the corresponding user's online access. A "Logout" request contains the attribute `COMMAND="RADIUS_LOGOUT"`.

The XML interface can process the following XML elements for a request:

☐ `SUB_USER_NAME`

User name

If the device receives this request and the Public Spot module discovers that this user is online with the corresponding MAC, then this user is logged out.

☐ `SUB_MAC_ADDR`

MAC address of the user's device Possible formats include:

- 00164115208c
- 00:16:41:15:20:8c
- 00-16-41-15-20-8c

☐ `TERMINATION_CAUSE`

Reason for the user to log off

The XML interface then sends the gateway a "Logout" response, which can contain the following XML elements:

☐ `SUB_USER_NAME`

User name

☐ `SUB_STATUS`

The current user status. The following values are possible:

- `RADIUS_LOGOUT_DONE`:?Logout successful
- `RADIUS_LOGOUT_REJECT`:?Logout rejected

☐ SUB_MAC_ADDR

MAC address of the user's device Possible formats include:

- 00164115208c
- 00:16:41:15:20:8c
- 00-16-41-15-20-8c

☐ TERMINATION_CAUSE

Reason for blocking access

Some examples of XML files are given below:

☐ **Logout-Request**

The external gateway sends the command for ending a session to the Public Spot:

☐
```
<?xml version="1.0" encoding="ISO-8859-1"?>
<PUBLICSPOTXMLINTERFACE>
??<ACCESS_CUBE COMMAND="RADIUS_LOGOUT">
????<SUB_USER_NAME>user2350</SUB_USER_NAME>
????<SUB_PASSWORD>5juchb</SUB_PASSWORD>
????<SUB_MAC_ADDR>00164115208c</SUB_MAC_ADDR>
????<TERMINATION_CAUSE>Check-Out</TERMINATION_CAUSE>
??</ACCESS_CUBE>
</PUBLICSPOTXMLINTERFACE>
```

☐ **Logout-Response:**

The XML interface sends a confirmation about the end of a session to the external gateway:

☐
```
<?xml version="1.0" encoding="ISO-8859-1" ?>
<PUBLICSPOTXMLINTERFACE>
??<ACCESS_CUBE ID="WLC-4006_PM" IP="192.168.100.2"
COMMAND="USER_STATUS">
????<SUB_STATUS>RADIUS_LOGOUT_DONE</SUB_STATUS>
```

```
????<SUB_MAC_ADDR>00:16:41:15:20:8b</SUB_MAC_ADDR>
????<SUB_USER_NAME>user2350</SUB_USER_NAME>
????<TERMINATION_CAUSE>User logout request</TERMINATION_CAUSE>
??</ACCESS_CUBE>
</PUBLICSPOTXMLINTERFACE>
```

Status

The external gateway queries the current status of a user from the Public Spot with a "Status" request. A "Status" request contains the attribute `COMMAND="RADIUS_Status"`.

The XML interface can process the following XML elements for a request:

☐ `SUB_USER_NAME`

User name

☐ `SUB_MAC_ADDR`

MAC address of the user's device Possible formats include:

- 00164115208c
- 00:16:41:15:20:8c
- 00-16-41-15-20-8c

The XML interface then sends the gateway a "Status" response, which can contain the following XML elements:

☐ `SUB_USER_NAME`

User name

☐ `SUB_MAC_ADDR`

MAC address of the user's device Possible formats include:

- 00164115208c
- 00:16:41:15:20:8c
- 00-16-41-15-20-8c

☐ `SUB_STATUS`

The current user status. The following values are possible:

- RADIUS_STATUS_DONE:?Status request successful
- RADIUS_STATUS_REJECT:?Status request rejected, e.g. unknown user or MAC address

☐ SESSION_TXBYTES

Current sent data volume

☐ SESSION_RXBYTES

Current received data volume

☐ SESSION_TXPACKETS

Number of data packets sent so far

☐ SESSION_RXPACKETS

Number of data packets received so far

☐ SESSION_STATE

Current status of the session

☐ SESSION_ACTUAL_TIME

Current time

Some examples of XML files are given below:

☐ **Status-Request**

The external gateway sends the command for a status request to the Public Spot:

☐
```
<?xml version="1.0" encoding="ISO-8859-1"?>
<PUBLICSPOTXMLINTERFACE>
??<ACCESS_CUBE COMMAND="RADIUS_STATUS">
????<SUB_USER_NAME>user2350</SUB_USER_NAME>
????<SUB_MAC_ADDR>00164115208c</SUB_MAC_ADDR>
??</ACCESS_CUBE>
</PUBLICSPOTXMLINTERFACE>
```

☐ **Status-Response:**

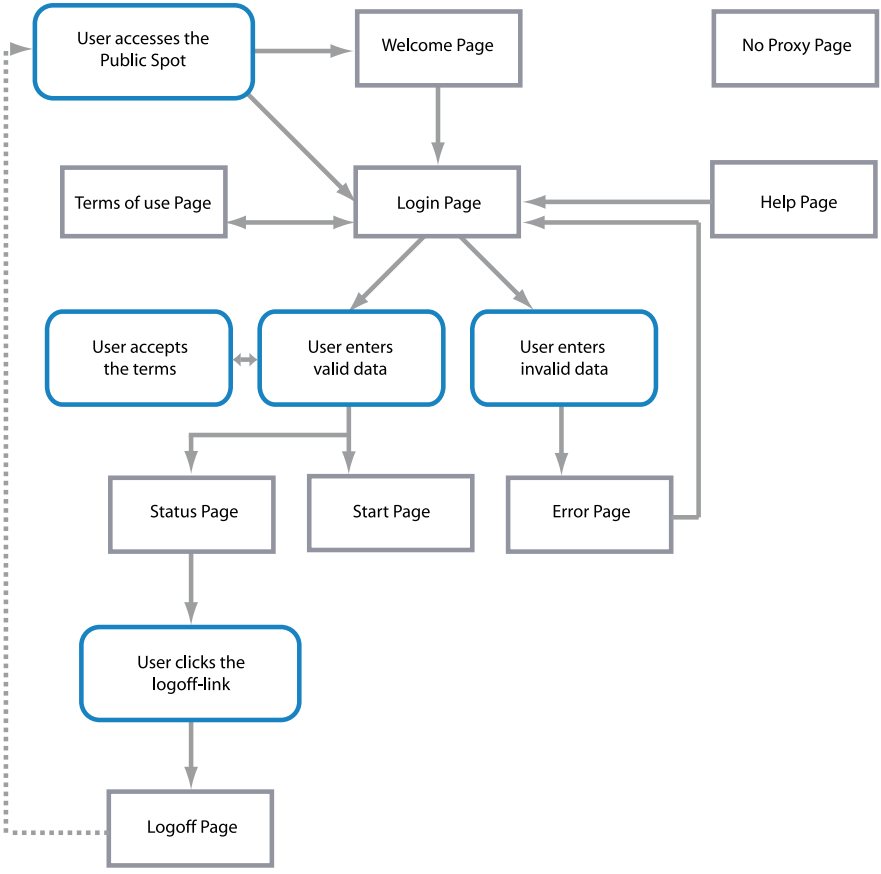
The XML interface sends a status message to the external gateway:

☐
```
<?xml version="1.0" encoding="ISO-8859-1" ?>
<PUBLICSPOTXMLINTERFACE>
??<ACCESS_CUBE ID="WLC-4006_PM" IP="192.168.100.2"
COMMAND="USER_STATUS">
????<SUB_STATUS>RADIUS_STATUS_DONE</SUB_STATUS>
????<SUB_MAC_ADDR>00:16:41:15:20:8b</SUB_MAC_ADDR>
????<SUB_USER_NAME>user2350</SUB_USER_NAME>
????<SESSION_ID>2</SESSION_ID>
????<SESSION_TXBYTES>0</SESSION_TXBYTES>
????<SESSION_RXBYTES>0</SESSION_RXBYTES>
????<SESSION_TXPACKETS>0</SESSION_TXPACKETS>
????<SESSION_RXPACKETS>0</SESSION_RXPACKETS>
????<SESSION_STATE>Authenticated</SESSION_STATE>
????<SESSION_ACTUAL_TIME>0</SESSION_ACTUAL_TIME>
??</ACCESS_CUBE>
</PUBLICSPOTXMLINTERFACE>
```

5.8 Default and Customized Authentication Pages

By default, your device uses pre-installed templates for the login page and all other authentication pages that your user sees before, during and after a Public Spot session. However, you do have the option of adapting the individual web pages to your requirements and changing the design. You need basic HTML knowledge of DIV containers and cascading style sheets (CSS), in order to effectively change the structure and layout of the individual pages.

The following flow-chart shows an overview and interaction of all available authentication pages on your device:



5.8.1 Available Pages

The „Welcome“ and „Login“ pages are displayed to users when they access the Internet or the Public Spot for the first time. The welcome page has a higher priority than the login page and is often used for cosmetic reasons only: Some hotspot providers like to welcome their users on a separate welcome page in order to present, for example, information about local offers

or instructions for registration, while others prefer to provide the fastest possible access to the Internet. Alternatively, some providers use the welcome page to display customized conditions of use, which users have to accept before they can go to the start page with the login form (e.g., "Login with name and password") or access the Internet ("Login after agreement").

This has nothing to do with the „Conditions of use“ page. This is displayed on the login page as an additional link if you selected login via e-mail or SMS, and if you also require confirmation of the conditions of use.

Hinweis: The pre-installed default pages on your device do not include a welcome page or the conditions of use. If you invoke one of these pages without loading the corresponding template onto your device, your users will automatically be redirected to the login page (missing welcome page) or an error message will be displayed (missing conditions of use).

After the user has logged in with his login data, the device checks that the information is correct and displays either an „Error“ page, which sends the users back to the login page, or shows the „Start“ page. This page verifies the successful login and redirects the user after a few seconds to the Internet page that the user originally requested. Additionally, a small popup window is opened that holds the „Status“ page. This page shows the user the current information about his session (e.g., time used so far, sent/received data volumes, and validity period for his account). It also offers a link to close the session and stop accounting. If a user clicks on this link, the user is sent to the „Logoff“ page, which confirms the successful logout from the Public Spot.

The remaining „Help“ and „No-proxy“ pages are isolated pages not related to the remaining login process.

- The „No-proxy“ page is displayed whenever a user tries to connect via HTTP on port 8080 instead of port 80. This port is typically used in Intranets for an HTTP proxy. Since this proxy is configured with a static IP address in the browser settings, but these can not be configured via DHCP, the user would not be able to reach this proxy in any case. The purpose of this page is just to instruct the user to disable the proxy before the user can proceed.
- The „Help“ page is only a placeholder in order to represent specific information (e.g., details about the login or where to get vouchers). The set of default pages built into the device does not contain a help page.

The „Voucher“ page is not one of the authentication pages: This is the graphic template for printing the vouchers. By uploading your own template, you can print tickets with the corporate design of your own company.

5.8.2 Pre-installed Default Pages

As mentioned previously, your device contains a set of pre-installed pages on delivery, which you can use to setup an operational Public Spot. There are pages for

- HTTP redirection,
- Login/logout function,
- Status Information.

They were deliberately designed to be simple, not to use any fancy features like dynamic HTML, and just present the necessary elements as-is. By only using the absolutely necessary elements, the correct display in any browser and any size of screen can be assured.

As the operator of a hotspot you may want to design more sophisticated pages or display a more neutral page without the manufacturer's logo. For that reason, the Public Spot module offers you the possibility to replace all or some of the default pages with your own design. This can be done either by using HTTP redirection or templates that you upload to the device and that the device processes like an intelligent HTML pre-processor. The templates can be directly loaded in the flash storage, which makes it possible to dispense with an external HTTP server (see page 380 „User-defined Pages Via HTTP Redirect“).

5.8.3 Configuration of User-defined Pages

If you would like to replace the pre-installed pages with your own webpages, you can either store them directly on the device or on an external HTTP server. Sophisticated HTML pages may require more storage space than the space available on the device. There are additional advantages when using websites from an external server:

- Changes can be applied centrally. This reduces the effort required to change the login pages when using several devices.
- The server can dynamically provide the pages whose appearance is influenced by the information that the device provides. This information is discussed in more detail in the following chapters.

The storage location for the templates is entered in LANconfig in `Public Spot:Public Spot:Page table:<Name of the template>:Page address (URL)`. There are currently three protocols available for the URL:

- `http://?`: Fetch the page via HTTP from an external server. TCP-port overrides and user/password specifications are possible.
- `https://?`: Similar to HTTP, but use HTTP over SSL for an encrypted connection.
- `file://?`: Retrieve the template from the given file in the device?s local file system.

You can use any file. Some file names are reserved for this purpose:

Tab. 1: Overview of the reserved file names for template pages

Local URL on your device	Page designation
file://pbspot_template_welcome	Welcome?
file://pbspot_template_login	Login...
file://pbspot_template_error	Error...
file://pbspot_template_start	Start?
file://pbspot_template_status	Status?
file://pbspot_template_logoff	Logoff...
file://pbspot_template_help	Help...
file://pbspot_template_noproxy	No proxy
file://pbspot_template_voucher	Voucher?*
file://pbspot_template_agb	Conditions of use...

*Template for printing vouchers, no authentication page

Hinweis: By uploading user-defined webpages, only the webpages that are pre-installed on the device are replaced, but not overwritten. They can be rolled back to the device's proprietary default pages at any time by deleting the local URL.

Hinweis: To provide the highest possible compatibility with earlier display devices and web browsers, you should avoid using frames, if possible. Also, specialized content such as JavaScript or plug-in elements can lead to an erroneous display.

5.8.4 URL Placeholder (Template Variables)

The URLs specified in the page table do not need to be absolute strings. You have the option to integrate template variables in the address which are then filled-out with parameters from a Public Spot session when the device requests the pages from the server. Placeholders have a form similar to C format strings, e.g., a percent sign immediately followed by a single, lowercase character. The following placeholders are defined:

☐ **%a**
Inserts the device?s IP address. The placeholder only returns a value if the „Request type“ in the „Page table“ is set to `Template`.

Hinweis: Note that this placeholder cannot generate a reachable address if the device itself is located behind another router with activated NAT.

☐ **%e**
Inserts the device serial number.

☐ **%i**
Inserts the NAS port ID. In this context, 'NAS' stands for 'Network Access Server'. This variable contains the interface of the device that the client used to login. For a WLC or router without WLAN this corresponds to a physical interface, such as `LAN-1`, or, for a standalone access point, it is the SSID.

☐ **%l**
Inserts the device host name.

☐ **%m**
Inserts the MAC address of the client as a hexadecimal string of length 12. The individual bytes are separated by colons.

☐ **%n**
Inserts the name of the device the way it is configured in the setup menu under „Name“.

☐ **%o**
Inserts the URL of the Internet page which the user initially requested. After successful authentication, the device forwards the user to this URL.

☐ **%s**

If the client is connected to the device via a WLAN interface, this placeholder will insert the WLAN SSID used in the network that the client is connected to. This feature is particularly interesting when MultiSSID is used, since this gives the server the opportunity to display different pages based on the SSID. If the client is connected via another access point that connects to the device via a Point-2-Point connection, the SSID of the first WLAN will be inserted. If the client is connect via Ethernet, the placeholder remains empty.

- **%t**
  Inserts the routing tag which is appended to the client's data packets.

- **%v**
  If the requesting client is assigned an individual VLAN ID, this variable contains the source VLAN ID.

- **%0-9**
  Inserts a single number between 0 and 9.

- **%%**
  Inserts a single percent character.

In order to be able to use variables for a template, add the parameters to the „Page Address (URL)“ in the page table. In the following URLs the variable `%i` is replaced with `LAN-1` as described in the sample above:

Example: `http://192.168.1.1/welcome.php?nas=%i`

Example: `http://192.168.1.1/%i_welcome.html`

5.8.5 User-defined Pages Via HTTP Redirect

If you implement user-defined pages with redirection (request type: redirect), your device transforms it as follows: Whenever your device must send the respective page to a client, it will expand the URL according to the rules given in the previous chapter and will send an HTTP 307 (temporary redirect) response to the device, with this URL as the new location.

Redirects are particularly meaningful if you use a welcome page and all authentications should be performed on one external gateway. In this case, the clients can be immediately redirected to this gateway. This feature is often used with the external device controller.

5.8.6 User-defined Pages Via Page Templates

The device can alternatively act as a client and use the extended URL to download a user-defined page via an HTTP connection. The internal pre-processor takes of the processing of the page and subsequently sends the result to the Public Spot user. This pre-processor makes it possible to process session-specific data, although the server has a static page available. The URL syntax understood by the device?s built-in HTTP client is the syntax recognized by web browsers. However, only a subset of what is recognized by browsers is supported: Usage of symbolic names for the server?s host instead of plain IP addresses is supported, given that DNS is properly configured. In many aspects, this mechanism can be considered like a proxy, which fetches HTML pages and then sends them to the client. The biggest difference is that the URL of the pages is determined by the device and not by the client of the Public Spot user.

- The user authentication is performed using the form `user:password@host/...`
- The device is incapable of automatically resolving non-fatal HTTP errors such as redirects. Make sure that an access to this page will return the page directly.

·■ Auto-fallback

For every entry in the page table, it is possible to individually define whether a fallback should be used or not. This fallback feature is only meaningful if a page is defined as a template (request type: template), and not as a redirect (request type: redirect). While fetching a page via HTTP, various errors can appear:

- The DNS lookup for a host name may fail.
- The TCP/HTTP connection to the server may fail.
- The HTTP server may respond with an error code (e.g. 404 if an invalid URL was given).

By default, the device passes this type of error on to the user so that the user can start a new request or inform the provider of the Public Spot. Alternatively, the configuration of a fallback feature can ensure that the hotspot continues to function by using the default pages instead. You enable the fallback feature in LANconfig using the setting „Fallback to implemented page“.

Passed HTTP Attributes

As mentioned above, in some respects the device may be seen as an HTTP proxy that fetches login and status pages for the client. HTTP proxies are obliged to keep certain HTTP attributes intact while forwarding a client request:

- The device forwards cookies between the client and the server. Client cookie values can also be sent transparently to the server and the server can set cookies on the client. Using cookies is necessary if the files that are sent from the server have ASP scripts, since ASP stores the session ID in a cookie.
- The device will forward the `User-Agent` value provided by the client. This allows a server to deliver different pages, based on the browser and system platform on the client side. PDAs and mobile phones for example call for web pages optimized for their small displays.
- The device inserts an `X-Forwarded-For` line into the HTTP request to report the device?s IP address.
- WEBconfig generally attempts to use a tag named `Accept-Languages` provided by client browsers to match the request to one of the languages provided by its internal message tables (currently, only German and English). The selected language is communicated to the server via another `Accept-Languages` tag, in the hope that the server will provide a page in the appropriate language. When the server delivers the page, the device will check for a Language tag in the server?s response to see if the server was actually capable of delivering a page in the requested language. If not, it will adapt the strings used in template expansion (see next section) to the actual language of the page.

5.8.7 Page Template Syntax

After the device receives the page from the server, it performs some transformations to the page template before sending it to the client. These transformations replace pre-defined HTML tag placeholders with data belonging to the client?s current session (e.g. the current resource consumption in the status page). An HTML page delivered by the server could therefore better be described as a template for an actual HTML page displayed in the client?s browser. HTML syntax was chosen for the placeholders to allow editing of page templates without interfering with syntax sensitive HTML editors.

In total, three placeholder tags are defined:

- `<pblink identifier>text</pblink>`

  Marks **text** as a clickable link to an **identifier**, typically to link to another page. Note that `</pblink>` is just an alias for `</a>`, since this symmetrical definition causes less trouble with HTML syntax checkers. For example, the following fragment defines a link to the help page:

- `Please click <pblink helplink>here</pblink>for help.`

- `<pbelem identifier>`

  Inserts the item specified by **identifier** at this location. For example, the following line inserts the user's time credit:

- `Session will be ended in <pbelem sesstimeout>.`

- `<pbcond identifier(s)>code</pbcond>`

  Only insert **code** into the page if all the identifiers are TRUE, i.e. numeric values are not equal to zero and string values are not empty. Note that the current implementation does not allow nested conditionals. Continuing from the previous example, the session timeout is only displayed if there is a time limit (a session without timeout internally has a session timeout of zero):

- ```
  <pbcond sesstimeout>Session will be terminated in <pbelem
  sesstimeout>seconds.</pbcond>
  ```

5.8.8 Page Template Identifiers

The following identifiers are currently defined.

Hinweis: Please note that not all identifiers are available for all printouts! Not all identifiers are available on all pages.

☐ **APADDR**
Valid for:`<pbelem>`
This identifier contains the Public Spot?s IP address, as seen from the client?s perspective. Can be used for user-defined login forms when the `LOGINFORM` element is not used.

☐ **HELPLINK**
Valid for:`<pbelem>`
This identifier contains the URL to the help page provided by the device.

☐ **LOGINERRORMSG**
  ```

Valid for:<pbelem>
This identifier returns the error message from LCOS in the case of a failed authentication. It is only valid when used on the error page.

Hinweis: To retrieve the error message from the RADIUS server in the event of a failed authentication, use the identifier **SERVERMSG**.

☐ **LOGINFORM**
Valid for:<pbelem>
This identifier refers to the HTML form for entering the user?s name and password.

☐ **LOGINLINK**
Valid for:<pbelem>
This identifier contains the URL to the login page provided by the device.

☐ **LOGOFFLINK**
Valid for:<pbelem>
This identifier contains the URL to the logout page provided by the device.

☐ **ORIGLINK**
Valid for:<pbelem><pblink><pbcond>
This identifier contains the URL originally requested by the user prior to the authentication process. If it is unknown, this value is empty.

☐ **REDIRURL**
Valid for:<pbelem><pblink><pbcond>
This identifier holds a possible redirection URL contained in the RADIUS server?s authentication response (if there was one). It is only defined for the error and start page.

☐ **RXBYTES**
Valid for:<pbelem>
This identifier contains the amount of data so far received by the device from the client in this session, expressed in bytes. It is zero for a station that is not logged in.

☐ **RXTXBYTES**
Valid for:<pbelem>
This identifier contains the amount of data received by the device from the client so far, or sent to the client in this session, expressed in bytes. This means that it is the sum of TXBYTES and RXBYTES.

☐ **SERVERMSG**
Valid for:<pbelem><pbcond>

This identifier holds the reply message contained in the RADIUS server?s authentication response (if there was one). Only applicable for the error and start pages. In the case of a failed authentication, this identifier contains the error message from the RADIUS server.

Hinweis: To retrieve the error message from the LCOS server in the event of a failed authentication, use the identifier **LOGINERRORMSG**.

☐ **SESSIONSTATUS**
Valid for:`<pbelem>`
This identifier contains a textual representation of the current status of the client relative to the device (whether authenticated or not).

☐ **SESSIONTIME**
Valid for:`<pbelem>`
This identifier contains the time that has passed since the login on the Public Spot.

☐ **SESSTIMEOUT**
Valid for:`<pbelem><pbcond>`
This identifier contains the remaining time for the current session. After this time, the device ends the current session automatically. This identifier is zero for a session with no time limit.

☐ **STATUSLINK**
Valid for:`<pbelem><pblink>`
This identifier contains the URL to the logout page provided by the device. A reference that opens a new browser window is automatically generated within the `<pblink>` element.

☐ **TXBYTES**
Valid for:`<pbelem>`
This identifier contains the amount of data transmitted by the device to the client so far in this session.

☐ **USERID**
Valid for:`<pbelem>`
This identifier contains the user ID with which the current session was started. The identifier is not specified if the client is not (yet) logged in.

☐ **VOLLIMIT**
Valid for:`<pbelem><pbcond>`
This identifier contains the amount of data, expressed in bytes, that the client is still allowed to transfer before the device terminates the current session. This identifier is zero for a session with no data limit.

5.8.9 Graphics in User-defined Pages

All but the simplest web pages contain images, which are fetched by the client?s browser independent of the HTML page itself. The graphic files for the pre-installed page are also stored on the device. The device automatically adapts the necessary permissions so that even unauthorized clients have access to the images without problems. However, every access to the referenced (device-external) images for user-defined pages are treated like a normal Internet access, and would automatically send the user back to the welcome or start page.

In order to avoid this behavior, you should make sure that the servers where the graphics are stored are included in the **free servers**. Free servers are addresses that have unlimited access, and are therefore also accessible by unauthenticated clients, and are not billed by the accounting feature in the same way as the rest of the data traffic.

The chapter on page 337 „Open Access Networks (No Login)“ contains further information on how to configure a free server. Note that if a user-defined page is defined as a redirect, this of course has to be defined as a free IP address.

5.9 Access to the Public Spot

5.9.1 Requirements for Logging In

- Device with network adapter
- Operating systems supporting the TCP/IP protocol (automatic IP-address retrieval by DHCP active)
- Web browser (supporting JavaScript and Frames)
- Direct Internet access (use of proxy deactivated)
- WLAN access information (network name, encryption information)
- Valid user data (user identifier and password)

Information for WLAN Access

A maximum of two pieces of information are required to access the WLAN:

- **The network name of the WLAN (SSID)**

  If the Public Spot's base stations are configured for operation as a closed network, the user must know the exact name of the wireless LAN, its SSID.

- **Wireless LAN encryption**

  Although it is possible to provide guest access via encrypted connections using, for example, WPA, Public Spots are not generally operated with WLAN encryption. Protection is provided in this case using authentication with a username and password. Data security when transmitting data on the Public Spot must be provided by the end user (e.g., using a VPN client).

Information for LAN access

If the IP addresses on your network are automatically assigned (for example, via DHCP), your users only need:

- a LAN socket that connects to the Public Spot.
- a LAN cable to connect their LAN adapter to the LAN socket.

Information for authentication

The user needs to have the following information to hand when logging in:

- User identifier
- Password
- MAC address

  If you set the authentication mode for a Public Spot at the base station to "MAC+User+Password", you, as the operator, must know the MAC addresses of the end devices employed by your users. An end device automatically and continuously transmits its MAC address when communicating with a base station. The user does not have to manually enter this information when logging in, but instead it is communicated just once to the operator before attempting to login.

5.9.2 Logging in to the Public Spot

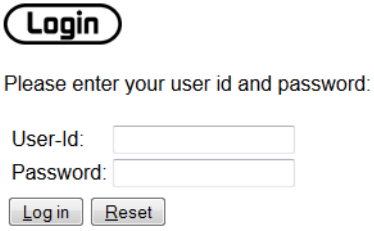
☐ Log in to the WLAN of the Public Spot (for WLAN connections) or connect to the network using an Ethernet cable (for LAN connections).

The different types of mobile devices and WLAN adapters offer various ways of entering the settings required for accessing the WLAN. Many devices require the network name (SSID) of the WLAN to be entered into the configuration program for the WLAN adapter. Some other products also provide an overview of all base stations in the vicinity, from which the user simply chooses the one they want to use.

Depending on the configuration, the user receives the necessary settings for the LAN-adapter connection either automatically from the network or a connected DHCP server, or from the network administrator.

☐ Start your Web browser.

As soon as the Web browser attempts to access any Internet site, the Public Spot automatically intervenes and presents the login page.



Hinweis: Depending on the firmware version, the actual login page may vary from the one shown here. However it looks, the login page will always present the input fields for user ID and password.

☐ Enter the complete „user ID“ and „password“ in the corresponding fields and confirm your entries with „Login“.

If the login to the Public Spot is successful, an additional window pops up with the main information about the current session. This window is also used for the login. This window should be left open throughout the session (e.g., it can be minimized).

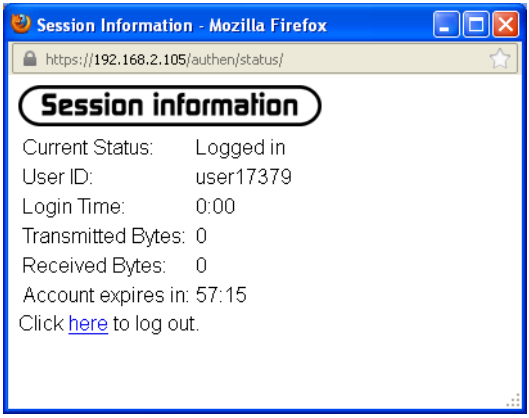
Hinweis: To login, you should use a Web browser with JavaScript support enabled to ensure that session status information can be displayed in a popup window.

5.9.3 Session Information

The window with session information is automatically updated at regular intervals. Along with the status and current user ID, the information displayed includes the connection time and the volume of transferred data.

If the session-information window is not open, you can open it by entering the following in the address line in the browser:

```
http://<IP address of the Public Spot>/authen/status/
```



5.9.4 Logging out of the Public Spot

The session information window can be used to logout from the Public Spot. Simply click on the word „here“ in the bottom line of text in the window.

If the session-information window is not open, you can enter the following into the address line in the browser:

```
http://<IP address of the Public Spot>/authen/logout
```

The Public Spot operator can supply you with the `<Public Spot's IP address>` upon request.

Hinweis: The operator can set up the Public Spot to automatically logoff users if they cannot be reached for 60 seconds. In case of doubt, please ask the Public Spot operator if automatic logoff (Station monitoring) is activated.

5.9.5 Advice and Help

The following sections present solutions to the most common problems that may occur when operating a Public Spot.

The Public Spot Login Page is Not Displayed

- The Internet access must be set up so that it is directed via the network adapter and not via a dial-up networking connection. To check this, take a look at the connection settings for your Web browser. If you use Microsoft Internet Explorer, you must disable the dial-up configurations in `Tools:Internet Options:Connections` entered there.
- Internet access must be direct, i.e. without going via a proxy server. In Microsoft Internet Explorer, you can disable the use of a proxy server in the menu `Tools:Internet Options:Connections:LAN settings...`.
- If you are making the connection with a WLAN adapter: Ensure that your network adapter can in fact find the Public Spot. Your WLAN adapter gives you the option of searching for an access point.
- If you are making the connection with a WLAN adapter: Check if your network adapter has all of the necessary settings to access the Public Spot network:
  - You probably have to enter the network name for the WLAN.
  - When working with an encrypted Public Spots, you are also required to enter the corresponding WPA or WEP key.
- Check that your network adapter is set up for automatic retrieval of an IP address (DHCP). Your device should not have a fixed IP address.

Hinweis: If your network adapter is set up with a fixed IP address, adjusting it for automatic retrieval by DHCP may cause important configuration information to be lost. Ensure that you note all of the values listed in the network settings (IP address, standard gateway, DNS server, etc.).

Login Not Working

- Ensure that you enter the user data correctly and in full. Ensure that you use the correct capitalization for all entries.
- Is the CAPS-LOCK key activated on your device? This causes the capitalization to be reversed. Deactivate the CAPS-LOCK key and repeat the entry of your login data.
- The Public Spot operator may be checking more than just the user ID and password, but also the MAC address (physical address) of your network adapter as well. In this case, ensure that the Public Spot operator is informed of your correct MAC address.

It is No Longer Possible to Login

If the Public Spot breaks off communications after a number of login attempts have failed, you should deactivate your WLAN adapter for at least 60 seconds (or your entire device) or disconnect the LAN adapter from the network, and then try again.

The Session Information Window is Not Being Displayed

To display the session-information window, enter the following line into the address line of your Web browser:

```
http://<IP address of the Public Spot>/authen/status/
```

The Public Spot operator can supply you with the `<Public Spot's IP address>` upon request.

The Public Spot Requests a New Login for No Reason (WLAN)

When moving into the signal coverage area of another access point (roaming), it is necessary to login again. If you are located in the overlap area between two access points, you may even experience a change of connection between the two access points at regular intervals. The task of the roaming secret is to allow Public Spot sessions to be passed between access points without the user having to login again.

▶ LANconfig: `Public Spot:Users:Roaming Secret`

5.10 Commonly Transmitted RADIUS Attributes

The RADIUS client module was implemented on the basis of RFCs no. 2865 and no. 2866.

These specifications define various attributes, some of which are an absolute necessity and some of which are optional. The following overview shows which attributes are transmitted/processed in messages between RADIUS servers and base stations.

5.10.1 Messages to/from the Authentication Server

Transferred Attributes

As previously mentioned, your device transmits far more than just the username and password in a RADIUS request. RADIUS servers might choose to completely ignore these additional attributes, or only use a subset of these attributes. Many of these attributes are used for access to the server using dial-in, and are defined as standard attributes in the RADIUS RFCs. However, some important information for hotspot operation can not be represented with standard attributes. The additional attributes are therefore marked with the enterprise ID 2356.

Overview of the RADIUS attributes transmitted by the device to the authentication server

☐ **1**
User-Name
The name entered by the user.

☐ **2**
User-Password
The password entered by the user.

☐ **4**
NAS-IP-Address
IP address of your device.

☐ **6**
Service-Type Id 1
Type of service that the user requested. The value `1` stands for **Login**.

☐ **8**
Framed-IP-Address
IP address that was assigned to the client.

☐ **26**
Vendor 2356(LCS) Id 2
MAC address of the client if authentication using the MAC address is enabled. In contrast to the Calling-Station-Id, this value is transmitted as a 6-byte binary string. This attribute only exists for the login mode „Authenticate with name, password and MAC address“.

☐ **30**
Called-Station-Id
MAC address of your device

☐ **31**
Calling-Station-Id
MAC address of the client The address is given byte-wise in hexadecimal notation with separators (nn:nn:nn:nn:nn:nn).

☐ **32**
NAS-Identifier
Name of your device, if configured.

☐ **61**
NAS-Port-Type

Type of physical port over which a user had requested authentication.

- **ID 19** denotes clients from WLAN
- **ID 15** denotes clients from Ethernet

☐ **87**
NAS-Port-Id
Description of the interface over which the client is connected to your device. This can be a physical as well as a logical interface, such as `LAN-1`, `WLAN-1-5` or `WLC-TUNNEL-27`.

Hinweis: Consider that more than one client may be connected to one interface at a time, so that, unlike dial-in servers, port numbers are not unique for clients.

Processed Attributes

Your device evaluates the authentication response of a RADIUS server for attributes that it may possibly process further. Most attributes however only have a meaning if the authentication response was positive, so that they influence the subsequent session:

Overview of the RADIUS attributes processed by the device

☐ **18**
Reply-Message
An arbitrary string from the RADIUS server that may transport either a login failure reason or a user welcome message. This message may be integrated into user-defined start or error pages via the `SEVERMSG` element.

☐ **25**
Class
An arbitrary octet string that may contain data provided by the authentication/accounting backend. Whenever the device sends RADIUS accounting requests, they will contain this attribute as-is. Within an authentication response, this attribute can occur multiple times in order, for example, to transmit a string that is longer than 255 bytes. The device processes all occurrences in accounting requests in the order they appeared in the authentication response.

☐ **26**
Vendor 2356(LCS) Id 1
Trafficlimit

Defines the data volume in bytes after which the device automatically ends the session. This value is useful for volume-limited accounts. If this attribute is missing in the authentication response, it is assumed that no volume limit applies. A traffic limit of 0 is interpreted as an account which is principally valid, however with a used-up volume budget. The device does not start a session in this case.

☐ **26**
Vendor 2356(LCS) Id 3
LCS-Redirection-URL
This can contain any URL that is offered as an additional link on the start page. This can be the start page of the user or a page with additional information about the user account.

☐ **26**
Vendor 2356(LCS) Id 5
LCS-Account-End
Defines an absolute point in time (measured in seconds since January 1, 1970 0:00:00) after which the account becomes invalid. If this attribute is missing, an unlimited account is assumed. The device does not start a session if its internal clock has not been set, or the given point in time is in the past.

☐ **26**
Vendor 2356(LCS) Id 8
LCS-Public Spot-Username
Contains the name of a Public Spot user for auto-login. Auto-login refers to the table of MAC authenticated users who are automatically assigned usernames by the server.

☐ **26**
Vendor 2356(LCS) Id 8
LCS-TxRateLimit
Defines the maximum downstream rate in kbps. This restriction may be combined with the corresponding Public Spot function.

☐ **26**
Vendor 2356(LCS) Id 9
LCS-RxRateLimit
Defines the maximum upstream rate in kbps. This restriction may be combined with the corresponding Public Spot function.

☐ **27**
Session-Timeout

Defines an optional maximum duration of the session, measured in seconds. If this attribute is missing in the response, an unlimited account is assumed. A Session timeout of zero seconds is interpreted as an account which is principally valid, however with a used-up time budget. The device does not start a session in this case.

☐ **28**
Idle-Timeout
Defines a time period in seconds after which the device will terminate the session if no packets were received from the client. This value overwrites in the locally defined idle timeout under `Public Spot:Public Spot:Idle timeout`.

☐ **64**
Tunnel-Type
Defines the tunneling protocol which will be used for the session.

☐ **65**
Tunnel-Medium-Type
Defines the transport medium over which the tunneled session will be established.

☐ **81**
Tunnel-Private-Group-ID
Defines the group ID if the session is tunneled.

☐ **85**
Acct-Interim-Interval
Defines the amount of time between subsequent RADIUS accounting updates. This value is only evaluated if the RADIUS client does not have a local accounting interval defined, i.e. if you have not set an „Accounting update cycle“ for the Public Spot module.

Hinweis: Note that the LCS-Account-End and Session-Timeout attributes are mutually exclusive, and it therefore does not make sense to include both in the response. If both attributes are included in a response, the attribute that appears as the last one in the attribute list will define the session?s time limit.

5.10.2 Messages to/from the Accounting Server

Transferred Attributes

The set of RADIUS attributes transmitted to a RADIUS server in an accounting request is similar to the set of attributes transmitted in an authentication request. However, additional attributes specific to accounting will be added. The following attributes are present in all RADIUS accounting requests:

Overview of the RADIUS attributes transmitted by the device to the accounting server

- ☐ **1**
  User-Name
  Name of the account that was used for authentication.
- ☐ **4**
  NAS-IP-Address
  IP address of your device.
- ☐ **8**
  Framed-IP-Address
  IP address that was assigned to the client.
- ☐ **25**
  Class
  All class attributes that the RADIUS authentication server sent in its authentication response.
- ☐ **30**
  Called-Station-Id
  MAC address of your device
- ☐ **31**
  Calling-Station-Id
  MAC address of the client The address is given byte-wise in hexadecimal notation with separators (nn:nn:nn:nn:nn:nn).
- ☐ **32**
  NAS-Identifier
  Name of your device, if configured.
- ☐ **40**
  Acct-Status-Type

Request type which signals the start or stop of accounting, or an interim update. You will find more information on page 353 „Request Types“.

☐ **44**
Acct-Session-Id
A series of characters that uniquely identify the client. It consists of the MAC address of the network adapter, the login timestamp (measured in seconds since January 1, 1970 0:00:00), and the session counter that your device manages locally.

☐ **61**
NAS-Port-Type
Type of physical port over which a user had requested authentication.

- **ID 19** denotes clients from WLAN
- **ID 15** denotes clients from Ethernet

☐ **87**
NAS-Port-Id
Description of the interface over which the client is connected to your device. This can be a physical as well as a logical interface, such as `LAN-1`, `WLAN-1-5` or `WLC-TUNNEL-27`.

Hinweis: Consider that more than one client may be connected to one interface at a time, so that, unlike dial-in servers, port numbers are not unique for clients.

In the case of an accounting stop request or an interim update, the request contains the following additional attribute:

☐ **42**
Acct-Input-Octets
The sum of all data bytes received from the client in this session, modulo 2^{32}.

☐ **43**
Acct-Output-Octets
The sum of all data bytes sent to the client in this session, modulo 2^{32}.

☐ **46**
Acct-Session-Time
The total duration of the client's session in seconds.

Hinweis: If the session was ended due to an idle timeout, this value is reduced by the idle time.

- **47**
  Acct-Input-Packets
  The number of data packets that your device received from the client during the session.
- **48**
  Acct-Output-Packets
  The number of data packets that your device sent to the client during the session.
- **49**
  Acct-Terminate-Cause
  The reason for termination or the end of the accounting session. This is sent if **Acct-Status-Type** has the value `Start` or `Stop`.
- **52**
  Acct-Input-Gigawords
  The upper 32 bits of the sum of all data bytes received from the client during this session.
- **53**
  Acct-Output-Gigawords
  The upper 32 bits of the sum of all data bytes sent to the client during this session.
- **55**
  Event-Timestamp
  The elapsed time since this accounting request was submitted by the device, measured in seconds since January 1, 1970 0:00:00. This attribute is only present if your device?s real time clock contains a valid value.

Hinweis: Note that the RADIUS accounting only starts accounting after a client successfully logs in, i.e. the time needed for authentication is not recorded. The Traffic-Limit-Option (see page 333) allows you to limit the data traffic during the authentication phase. The final accounting stop request also contains the termination cause attribute (49).

Processed Attributes

Your device currently does not process any attributes in responses sent by a RADIUS accounting server.

6 Virtual Private Networks – VPN

6.1 What are the Benefits of VPN?

A VPN (Virtual Private Network) via IPSec enables you to establish secure connections from a remote PC to a OpenBAT device over the Internet (Remote Access Service - RAS).

Connection via the Internet

When the Internet is used instead of direct connections, the following structure results:

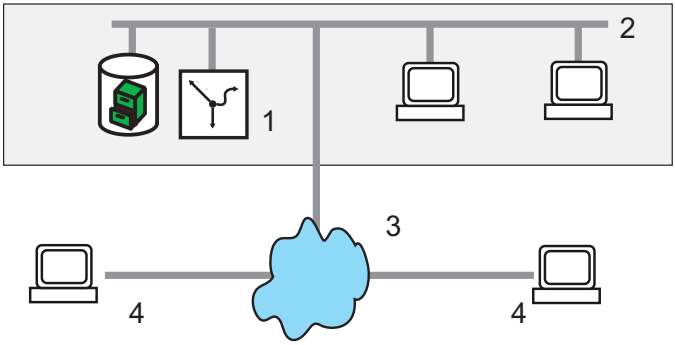


Figure 65: Connection via the Internet
1: OpenBAT device
2: LAN
3: Internet
4: Computer with remote-access connection

All participants are connected to the Internet (fixed or dial-in connection). There are no longer expensive dedicated lines between the participants.

- ☐ Only the Internet connection of the head office's LAN is necessary. Special dial-in devices or routers for dedicated lines to individual participants can be omitted.
- ☐ The RAS computers dial into the head office's LAN via the Internet.

There are no longer any direct physical connections between 2 participants, but each participant has direct access to the Internet. The access technology does not play a role here: Ideally, broad-band technologies, such as DSL (Digital Subscriber Line) in connection with flat rates are used.
It is not necessary that the technologies used by the individual participants are compatible, as is the case with conventional direct connections. Via a single Internet access you can establish several simultaneous logical connections to various remote stations.
Low connection costs and high flexibility make the Internet (or any other IP network) an excellent transfer medium for a corporate network.
Two technical characteristics of the IP standard, however, are detrimental to the use of the Internet as part of corporate networks:
☐ The necessity of public IP addresses for all participants.
☐ Insufficient data security due to unprotected data transmission.

6.1.1 Private IP Addresses on the Internet?

The IP standard defines two types of IP addresses: public and private addresses. A public IP address is valid worldwide, while a private IP address is only valid in an isolated LAN.
It is necessary that public IP addresses are unique worldwide. Private IP addresses can occur any number of times worldwide, but only once within an isolated LAN.
Usually, computers in the LAN only have private IP addresses, only the router that is connected to the Internet also has a public IP address. The computers behind this router access the Internet via its public IP address (IP masquerading). In such a case, solely the router itself is addressed via the Internet. There is no possibility to address computers behind the router without intervention by the router.

6.1.2 Security of Data Traffic on the Internet?

The skepticism towards the idea of handling parts of corporate communication over the Internet is based on the fact that the Internet is no longer within a company's direct sphere of influence. Unlike with dedicated connections, the data is transmitted through external network structures whose owners are unknown to the company.
In addition, the Internet is based on a simple form of data transmission using unencrypted data packets. Further participants through whose networks the packets are transmitted might read them or even manipulate them. Anyone can access the Internet. This entails the risk that additional participants also try to gain unauthorized access to the transmitted data.

- **VPN – Security based on Encryption**
  To resolve this security problem, encrypt the data traffic between two participants. While the data is transmitted in the VPN, it is unreadable to other participants.
  The latest and most secure cryptographic procedures are used for encryption. For this reason, the transmission security in the VPN exceeds the security level of dedicated lines by far.
  The participants agree on data-encryption codes which are referred to as "keys". These keys are only known to the persons involved in the VPN connection. Without a valid key, the data packets cannot be decrypted. The data is inaccessible to other participants, it remains 'private'. A direct connection between two remote terminals within the IPSec VPN is referred to as "transport mode".

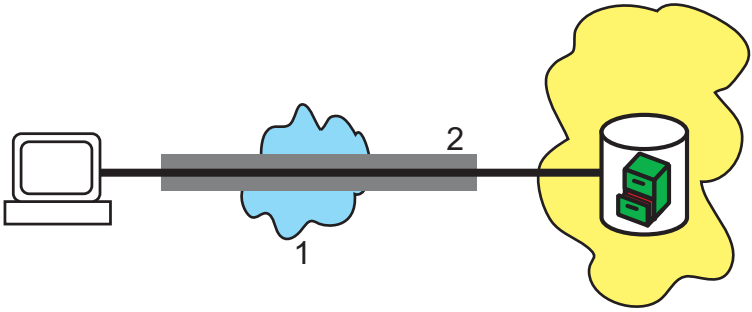


Figure 66: VPN data transmission in IPSec transport mode
1: Internet
2: VPN tunnel

- **Send your Data into the Tunnel – for Security Reasons**
  It now becomes clear why VPN creates a virtual private network: the devices never establish a fixed physical connection between each other. The data moreover follows suitable routes through the Internet. It is still harmless, however, if additional participants intercept and record the transmitted data during transmission. As the devices have encrypted the data by VPN, the actual content remains inaccessible. Experts compare this status to a tunnel: Open at the beginning and the end, but perfectly shielded in between. The most secure connections within a public IP network are therefore referred to as "tunnels". A connection between two networks within the IPSec VPN is referred to as "tunnel mode".

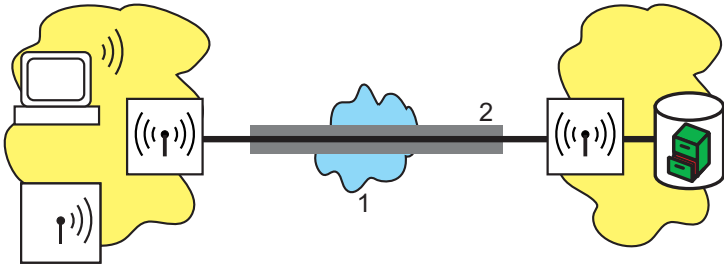


Figure 67: VPN data transmission in IPSec tunnel mode
1: Internet
2: VPN tunnel

The aim of modern network structures has thus been achieved: Provide secure connections over the largest and cheapest of all public IP networks: the Internet.

6.2 VPN at a Glance

6.2.1 VPN Application Example

You can use VPN connections in various different areas of application. Different transmission technologies for data and also audio are used, which VPN unites to an integrated network. The following example shows a typical application, which can often be found in practice in identical or similar form.

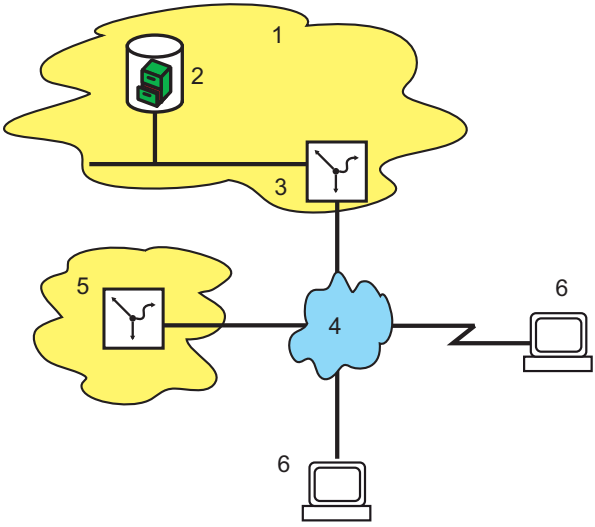


Figure 68: Application example of a VPN connection

1: Head office
2: Server in the DMZ
3: VPN gateway
4: Internet
5: Branch office
6: Computer with remote access connection

The essential components and characteristics of these applications:

- ☐ Coupling of networks, e.g. between the head office and the branch office
- ☐ Connection of branch offices without fixed IP addresses via the VPN router
- ☐ Connection of home offices without fixed IP, possibly via ISDN or analog modems
- ☐ Connection to Voice-over-IP telephone systems
- ☐ Connection of mobile users, e.g. via public WLAN access

6.2.2 VPN Functions

This section lists all VPN functions and features. Experts in the VPN sector are offered a highly compressed summary of the performance of the function. Understanding the terminology requires a sound knowledge of the technical fundamentals of VPN. However, for commissioning and normal operation of the LANCOM VPN, this information is not required.

- VPN based on IPSec standard
- VPN tunnel via leased-line connection, dial-up connection and IP network
- IKE main and aggressive mode
- IPSec protocols ESP, AH and IPCOMP in transport and tunnel mode
- Hash algorithms:
  - HMAC-MD5-96, hash length 128 bits
  - HMAC-SHA-1-96, hash length 160 bits
- Symmetrical encryption methods
  - AES, key length 128, 192 and 256 bits
  - Triple-DES, key length 168 bits
  - Blowfish, key length 128-448 bits
  - CAST, key length 128 bits
  - DES, key length 56 bits
- Compression using "deflate" (ZLIB) and LZS
- IKE Config Mode
- IKE using pre-shared keys
- IKE using RSA signature and digital certificates (X.509)
- Key exchange via Oakley, Diffie-Hellman algorithm with a key length of 768 bits, 1024 bits, 1536 bits and 2048 bits (well known groups 1, 2, 5 and 14)
- Key management according to ISAKMP
- Authentication via Extended Authentication Protocol (XAUTH)

6.3 Configuration of VPN Connections

The following three questions come up when VPN connections are configured:

- ☐ Between which VPN gateways (remote terminals) is the connection established?
- ☐ Which security parameters secure the VPN tunnel between both gateways?
- ☐ Which networks and computers communicate via this tunnel?

Note: This section describes the basic considerations for the configuration of VPN connections. First, a simple connection between two local networks is described. Descriptions of special cases, e.g. dialing into LANs using individual computers (RAS) or connecting structured networks can be found further down.

6.3.1 VPN Tunnel: Connection between VPN Remote Terminals

In virtual private networks (VPNs), you can connect local networks over the Internet. The device routes the private IP addresses from the LANs via an Internet connection between 2 VPN remote terminals with public IP addresses.
To enable secured routing of the private IP address ranges via the Internet connection, establish a VPN connection between the two LANs. This connection is also referred to as VPN tunnel.

The VPN tunnel has two important tasks:

- ☐ It shields transmitted data from unwanted access by unauthorized persons
- ☐ It forwards private IP addresses via an Internet connection over which only public IP addresses can be routed.

The following parameters define the VPN connection between the two gateways:

- ☐ The end points of the tunnel, the VPN gateways, which a device reaches via a public IP address (static or dynamic)
- ☐ The IP connection between the two gateways
- ☐ The private IP address ranges that the two VPN gateways are routing.
- ☐ Security-relevant settings, such as passwords, IPSec keys, etc. for shielding the VPN tunnel

This information can be found in the VPN rules.

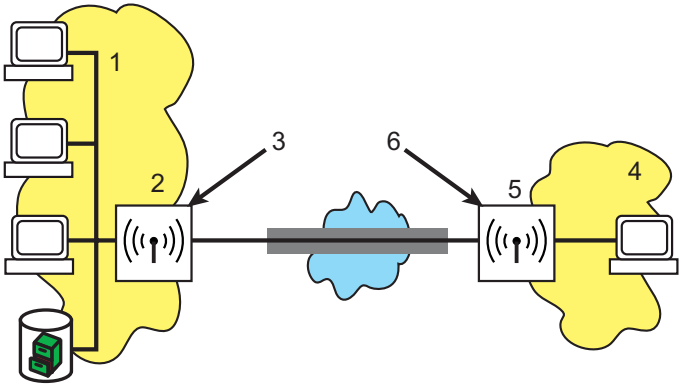


Figure 69: VPN tunnel between gateways

1: Private IP network: 10.1.0.0 Network mask: 255.255.0.0
2: Public IP address: 80.146.81,251
3: IP connection
4: Computer with remote access and dynamic IP address
5: VPN tunnel

6.3.2 1-Click VPN for LANCOM Advanced VPN Client

VPN access for employees who dial into a network by means of the LANCOM Advanced VPN Client can easily be created using the setup wizard. You can export them into a file which the LANCOM Advanced VPN Client imports as a profile. During this process, the client retrieves the required information for the current configuration from the Hirschmann VPN Router and adds randomly generated values (e.g. for the pre-shared key).

- ☐ Start the setup wizard ‘Set up access’ via LANconfig and select the ‘VPN connection’.
- ☐ Activate the options ‘LANCOM Advanced VPN Client’ and ‘Accelerate configuration with 1-click VPN’.
- ☐ Enter the name for this access and select under which address the router can be reached from the Internet.
- ☐ In a last step, select how the device outputs the new access data:
  - ▶ Save profile as import file for the LANCOM Advanced VPN Client
  - ▶ Send profile via e-mail
  - ▶ Print profile

Note: Sending the profile file via e-mail represents a security risk because someone could intercept the e-mail.

To send the profile file via e-mail, the device must be configured with an SMTP account including the necessary access data. Furthermore, the configuration computer must include an e-mail program that is set up as standard e-mail application and that other applications can also access for sending e-mails.

When generating the VPN access, the device uses settings that are optimally configured for use in the LANCOM Advanced VPN Client, among them, e.g..:

- ☐ Gateway: If defined in the BAT VPN Gateway, a DynDNS name is used, otherwise the IP address
- ☐ FQDN (Full Quality Domain Name): Combination of the name of the connection, a sequential number and the internal domain in the BAT VPN Gateway
- ☐ Domain: If defined in the BAT VPN Gateway, the internal domain is used, otherwise a DynDNS name or the IP address.

- ☐ VPN IP networks: All IP networks of the ‘Intranet’ type defined in the device.
- ☐ Pre-shared key: Randomly generated key with a length of 16 ASCII characters.
- ☐ Connection medium: The LAN serves to establish connections.
- ☐ VoIP prioritization: The VoIP prioritization is activated by default.
- ☐ Exchange mode: As exchange mode, the ‘aggressive mode’ is employed.
- ☐ IKE config. mode: The IKE config mode is activated, the IP address information for the LANCOM Advanced VPN Client is automatically assigned by the BAT VPN Gateway.

6.3.3 Viewing VPN Rules

As the VPN rules are always a combination of various pieces of information, you define these rules indirectly in a device. You do this by compiling them from different sources.
You can call up information on the current VPN rules in the device using the Telnet console. To do this, establish a Telnet connection to the VPN gateway and enter the following command in the console:

```
show vpn
```

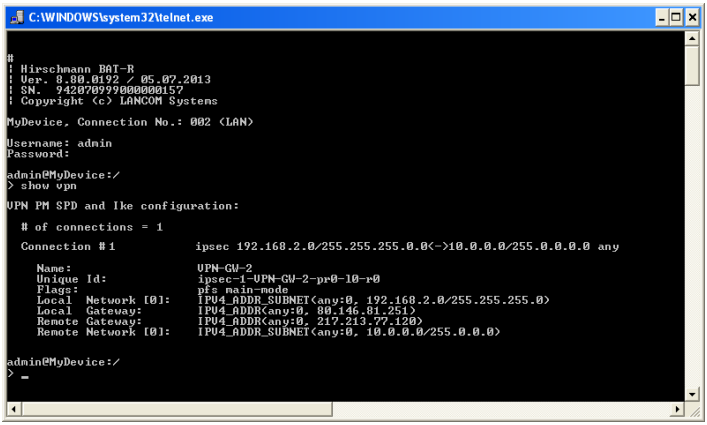


Figure 70: Calling up VPN rules using Telnet

The output contains information on the network relationships that are relevant for setting up VPN connections to other networks.
In this case, the local network of a branch office (network 192.168.2.0 with network mask 255.255.255.0) is connected to the network of the head office (network 10.0.0.0 with network mask 255.0.0.0). The public IP address of your own gateway is 80.146.81.251, the one of the remote VPN gateway is 217.213.77.120.
The following command shows the protocols and ports permitted over the connection:

```
any:0
```

An extended output can be requested using the command "show vpn long". In addition to the network relationships, this output also includes information on security-relevant parameters, such as IKE and IPSec proposals.

6.3.4 Manually Setting up VPN Connections

Manually setting up VPN connections involves the tasks previously described:

- ☐ Defining tunnel end points
- ☐ Defining security-relevant parameters (IKE and IPSec)
- ☐ Defining the VPN network relationships, meaning the IP address ranges to be connected. In case of overlapping IP network ranges on both sides of the connection, please also observe the section 'N:N mapping'.
- ☐ When coupling Windows networks (NetBIOS/IP): Without WINS servers on both sides of the VPN connection (e.g. when connecting home offices), the device assumes the corresponding NetBIOS proxy functions. This requires the activation of the NetBIOS module in the device and the entry of the corresponding VPN remote terminal as remote terminal in the NetBIOS module. If, however, both networks have their own WINS servers in the case of site-to-site connections, deactivate the NetBIOS module, so that the device no longer performs any NetBIOS proxy functions.

Note: To use the device's NetBIOS proxy, enter the IP address of the remote terminal (Intranet address) as primary NBNS in the IP parameter list. You will find the settings under LANconfig: Communication / Protocols.

Apart from your own, local VPN gateway, enter one VPN remote terminal each in the VPN connection list.

Manually configuring the VPN connections involve the following steps:

- ☐ Create an entry for the remote VPN gateway in the connection list and enter the public IP address.
- ☐ The device takes the security parameters for the VPN connection from the prepared lists. Apart from the definition of an IKE key, there is no further need for action.

- ☐ For a dynamic VPN connection, create a new entry in the PPP list with the name of the remote VPN gateway as remote terminal, the name of the local VPN gateway as user name and a suitable password. For this PPP connection, definitely activate the IP routing and, if required, also the routing of "NetBIOS over IP". Define the remaining PPP parameters, such as the procedure for checking the remote terminal, as with other PPP connections.
- ☐ The main task in setting up VPN connections is the definition of network relationships: Which IP address ranges on both sides of the VPN tunnel will you integrate into the secured connection?

6.3.5 IKE Config Mode

When configuring VPN dial-in access options, you can, as an alternative to the fixed assignment of IP addresses, also enter a pool of IP addresses for the remote terminals logging in. To do this, select the "IKE-CFG" mode in the entries of the connection list. It can take the following values:

- ▶ Server: With this setting, the device functions as server for this VPN connection. There are 2 possibilities for assigning the IP address to the client:
  - ▶ If there is an entry for the remote terminal in the routing table, the device assigns it the IP address configured there.
  - ▶ If there is no entry for the remote terminal in the routing table, the device takes a free IP address from the IP pool of the dial-in access options.

Note: Here it is necessary that you configure the remote terminal as IKE-CFG client and it thus requests an IP address for the connection from the server.

- Client: With this setting, the device functions as client for this VPN connection and requests an IP address for the connection from the remote terminal (server). The device thus behaves similar to a VPN client.
- Off: If the IKE-CFG mode is switched off, the device does not assign IP addresses for the connection. In this case it is necessary that you configure fixed IP addresses to be used for this connection on both sides of the VPN path.

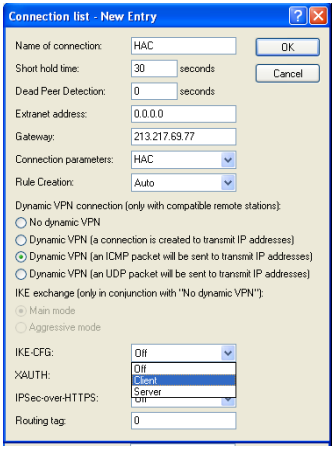


Figure 71: Editing an entry in the connection table

LANconfig: VPN / General / Connection list
WEBconfig: HiLCOS menu tree / Setup / VPN / Name list

6.3.6 Establishing VPN Network Relationships

With the integrated firewall, Hirschmann Routers include a powerful instrument for the definition of source and target address ranges. For this purpose, you can allow or deny data transmission (if required, with further limitations). Use this function also for setting up the network relationships for the VPN rules.

In the best case, the firewall generates the VPN rules automatically.

- As source network, the firewall uses the local Intranet, meaning the private IP address range which includes the local VPN gateway itself.
- As destination networks for the automatically generated VPN rules, the network areas from the IP routing table are used, with a remote VPN gateway as specified router.

To activate this automatic generation of rules, it is sufficient that you activate the corresponding option in the firewall. This is done automatically when the VPN installation wizard in LANconfig is used. When two simple local networks are coupled, the automatic VPN function derives the network relationship from the IP address range of its own LAN and from the entry for the remote LAN in the IP routing table.

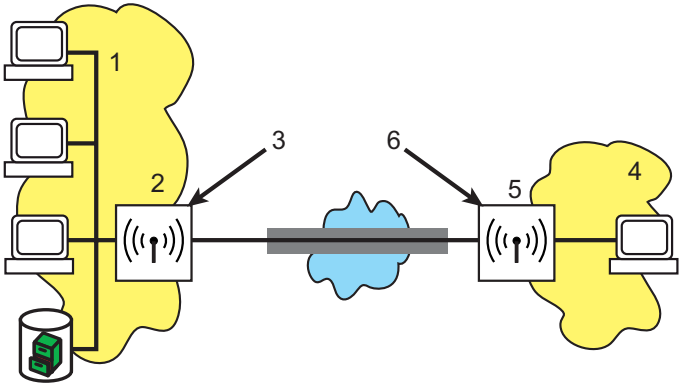


Figure 72: Automatic VPN function with coupled LANs
1: IP network: 10.1.0.0 Network mask: 255.255.0.0
2: VPN-GW-1: 80.146.81,251
3: IP routing table: 10.2.0.0/16 > VPN-GW-2
4: IP network: 10.2.0.0 Network mask: 255.255.0.0
5: VPN-GW-2: 217.213.77,120
6: IP routing table: 10.1.0.0/16 > VPN-GW-1

The description of the network relationships becomes more complex when the source and destination networks exceed the respective Intranet address range of the connected LANs.
If one part of the entire local Intranet connects to the remote network, the automatic function releases an IP address range for the VPN connection that is too large.
As they are connected to the local Intranet via additional routers, many network structures are connected to other network sections with their own IP address ranges. Include these address ranges in the network relationship using additional entries.
In these cases it is necessary that you manually enter the network relationships to describe the source and destination networks. Depending on the situation, this leads to an extension of the automatically generated VPN rules. It might be necessary to switch off the automatic VPN function completely in order to avoid unwanted network relationships.

Define the required network relationships using corresponding firewall rules under the following conditions:

- ☐ For the firewall rule, activate the option "This rule is used for generating VPN rules".
- ☐ As firewall action, select the option "transmit" in any case.
- ☐ You can enter individual stations, specific IP address ranges or entire IP networks as source and target for the connection.

Note: The firewall rules for the generation of VPN rules are active even when you do not require a firewall function in the device and have therefore deactivated it.

Note: Define the destination networks in the IP routing table, so that the router forwards the corresponding data packets in the devices to the other network. Use the already available entries and enter a higher-level network as target. The intersecting portion of the destination-network entry in the firewall and the subordinate entries in the IP routing table will be integrated into the network relationships for the VPN rules.

Example: The IP routing table contains the destination networks 10.2.1.0/24, 10.2.2.0/24 and 10.2.3.0/24, which are all connected via the VPN-GW-2 router. One entry for the destination network 10.2.0.0/16 in the firewall is sufficient to include the three desired subnetworks in the VPN rules.

Note: Define identical source and destination networks on both sides of the VPN connection. This is required if you map a larger target-address range onto a smaller source-address range at the remote terminal. Decisive are the IP address ranges allowed by the VPN rules, and not the networks specified in the firewall rules. These may deviate from the network relationships in the VPN rules because of intersecting ranges.

Depending on your requirements, you can additionally limit the VPN connection to specific services or protocols. This will permit you to e.g. reduce the VPN connection to use with a Windows network only.

Note: For this limitation, use separate rules that apply exclusively to the firewall and are not used for the generation of VPN rules. Firewall/VPN rules can quickly become complex and difficult to manage.

6.3.7 Collective Establishment of Security Associations

"Security Associations" (SAs) form the basis for establishing a VPN tunnel between two VPN remote terminals. An SA defines, among others, the following parameters:

- IP addresses of source and destination network
- Encryption, integrity check and authentication methods
- The key for the connection
- The period of validity of the keys used

The Security Associations are defined by automatically or manually generated VPN rules (see also 'Establishing VPN Network Relationships' in the reference manual).

Usually, an IP packet transmitted from the source network to the destination network triggers the establishment of Security Associations. In the case of keep-alive connections, this is an ICMP packet that the device sends to the remote terminal by an entry in the polling table.

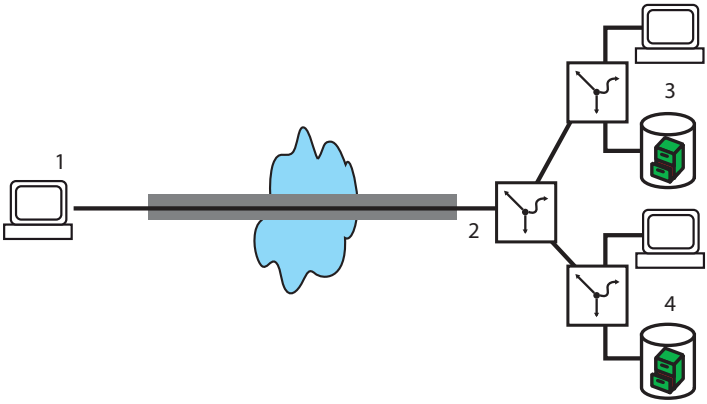


Figure 73: Various connected IP networks
1: Computer with remote access
2: IP network: 10.2.x.x
3: IP network: 192.x.x.x
4: IP network: 172.x.x.x

In complex network scenarios, various network relationships are possible between two VPN remote terminals. If the device transfers a single IP packet, this leads to the establishment of SAs for precisely this one network relationship which matches this packet. For the establishment of the other SAs, the device requires IP packets matching the other network relationships.
The establishment of SAs based on data packets requires time and leads to packet losses as long as the SAs are not yet installed. This is often an unwanted effect, especially with keep-alive connections. Instead, all SAs matching the network relationships defined in the remote terminal are established immediately. As the negotiation of all SAs requires substantial CPU performance particularly in complex scenarios, you can define the behavior with the parameter "Establish SAs collectively".

- Establish SAs collectively
  - Yes: The device establishes all defined SAs.
  - No [default]: The device only establishes the SAs explicitly addressed by a packet to be transmitted.
  - Only with keep alive: The device establishes all defined SAs for remote terminals with a hold time of '9999' (keep alive) in the VPN connection list.

WEBconfig: HiLCOS menu tree > Setup > VPN

Note: In most cases, the default setting for the exclusive establishment of explicitly addressed SAs is sufficient, especially if you are only using automatically generated VPN rules. The currently available SAs are listed under HiLCOS menu tree/Status/VPN.

6.3.8 VPN Connection Diagnostics

If the VPN connections fail to work after the relevant parameters have been configured, the following diagnostic methods are available:

- ☐ Use the command `show vpn spd` on the Telnet console to call up the "Security Policy Definitions".
- ☐ Use the command `show vpn sadb` to call up information about the negotiated "Security Associations" (SAs).
- ☐ Use the command `trace + vpn` to call up the status and error messages for the current VPN negotiation.
  - ▶ The error message `No proposal chosen` indicates a configuration error at the remote terminal.
  - ▶ The error message `No rule matched`, on the other hand, indicates a configuration error in the local gateway.

6.4 IPSec over HTTPS

6.4.1 Introduction

In some environments, it is impossible to establish a secured VPN connection over an existing Internet connection because the ports used by IPSec are blocked in the settings of an upstream firewall. To permit the establishment of an IPSec-secured VPN connection even under these conditions, the VPN routers support the 'IPSec over HTTPS' technology. The device initially tries to transmit data via standard IPSec. If the connection fails to be established (e.g. because IKE port 500 is blocked by a mobile phone network), an automatic attempt to set up a connection is made. For this attempt, the device encapsulates the IPSec VPN with an additional SSL header (port 443, as with https).
Please note that the 'IPSec over HTTPS technology' is only available when both remote terminals support this function and when the relevant options are activated. IPSec over HTTPS is available in VPN routers with HiLCOS 8.0.

6.4.2 Configuring the IPSec over HTTPS Technology

To actively establish a connection from a VPN device to another remote terminal using the IPSec over HTTPS technology, activate the option in the relevant entry for the remote terminal in the VPN name list.
LANconfig: VPN / General / Connection list
WEBconfig: Menu tree / Setup / VPN / VPN remote terminal

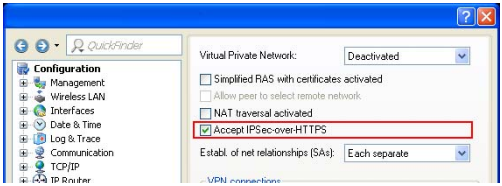


Figure 74: Configuring active IPSec over HTTPS

☐ IPsec-over-HTTPS: With this option, you activate the IPSec over HTTPS technology when actively establishing a connection to this remote terminal.

- Possible values: On, Off
- Default: Off

Note: With activated IPSec over HTTPS option, the VPN connection is only available when the remote terminal also supports this technology and when the acceptance of passive VPN connections with IPSec over HTTPS has been activated in the remote terminal.

For the passive establishment of a connection to a VPN device from another VPN remote terminal using the IPSec over HTTPS technology (e.g. LANCOM Advanced VPN Client), activate the option in the general VPN settings.
LANconfig: VPN / General
WEBconfig: Menu tree / Setup / VPN

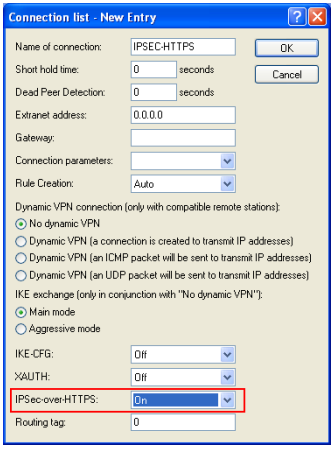


Figure 75: Configuring passive IPSec over HTTPS

☐ Accept SSL-IPsec: With this option, you activate the acceptance of passive connection setups when the remote terminal supports the IPSec over HTTPS technology.
- Possible values: On, Off
- Default: Off

Note: The LANCOM Advanced VPN Client supports automatic fallback to IPSec over HTTPS. With this setting, the VPN client first tries to establish a connection without additional SSL encapsulation. If the device fails to establish a connection, it then tries to establish a connection with the additional SSL encapsulation.

6.4.3 Status Displays for IPSec over HTTPS Technology

The status displays for every active VPN connection indicate whether the IPSec over HTTPS technology (SSL encaps.) is activated for the respective connection.
WEBconfig:Hirschmann Menu tree / Status / VPN / Connections

6.5 Use of Digital Certificates

The security of communications via VPN fulfills three core requirements:
- Confidentiality: No unauthorized person can read the transmitted data (via encryption).
- Integrity: No unauthorized person can change the data while it is being transmitted (via authentication – hash).
- Authenticity: The recipient ensures that the data received has really been sent by the supposed sender (via authentication).

A number of procedures are available for the encryption and authentication of data, providing satisfactory solutions for the first two aspects – confidentiality and integrity. The use of digital certificates aims at also ensuring the authenticity of the communication partners.

6.5.1 Basics

Encryption methods can be divided into 2 categories: Symmetrical and asymmetrical encryption.

Symmetrical Encryption

Symmetrical encryption has been known for thousands of years and is based on the fact that both the sender and the recipient of a message have a shared secret key. This key can take on various forms. The Romans used a stick of a certain diameter for encryption and decryption. In today's digital communication, the key is usually a specific password. Using this password and an encryption algorithm, the sender modifies the data to be sent. The recipient uses the same key and the relevant decryption algorithm to render the data readable again. Any other person who does not know the key cannot read the data. A common symmetrical encryption method is 3DES, for example.

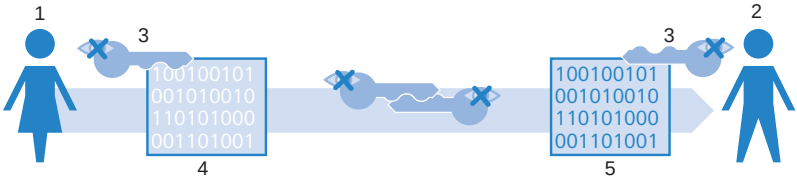


Figure 76: Symmetrical encryption method

1: Alice
2: Bob
3: Secret key
4: Encrypted message
5: Message in plain text

Example:

- ☐ Alice wants to send a confidential message to Bob. To do this, she encrypts the message with a secret key and a secret procedure, such as 3DES. She sends the encrypted message to Bob, informing him of the encryption method she has used.
- ☐ Bob has the same key as Alice. As he also knows the encryption method Alice used, he can decrypt the message and transform it back into plain text.

Symmetrical encryption is very simple and efficient, but has two significant disadvantages:

- ☐ Each secret communication relationship requires a separate key. If Carol joins Alice and Bob, three keys are necessary to secure the data communication between all partners, with four participants, six keys are required, with 12 participants, 66 and with 1000 participants, almost 500,000. In a worldwide network with ever increasing requirements for the secure communication of numerous participants, this becomes a serious problem.
- ☐ While this first disadvantage could be solved with technological means, the second problem remains the core problem for symmetrical encryption. On both sides of the data transmission, the secret key must be known and protected from unauthorized persons. If Alice simply e-mails the key to Bob, this method is not secure enough. The prerequisite is that the data connection is sufficiently secured, which is achieved precisely with this key. She must hand over the key to Bob in person or transmit it using an 'interception-proof' method. This task is difficult to handle in times of worldwide dynamic data communication.

Asymmetrical Encryption

Asymmetrical encryption was developed in the 70ies as a fundamentally new approach. Instead of one secret key that is known to both sides, this variant employs a pair of keys.

- The key owner uses the first part of the key pair to encrypt the data he is going to transmit. This key, subsequently referred to as public key, can be made publicly available to anyone worldwide.
- The second part of the key pair is the private key, which is only used for decrypting the messages received. Protect this secret key from access by unauthorized persons.

The main difference to symmetrical encryption methods: A publicly known key is used, resulting in the name "public-key method". A common asymmetrical encryption method is RSA, for example.
Let's take another look at the example of Alice and Bob:

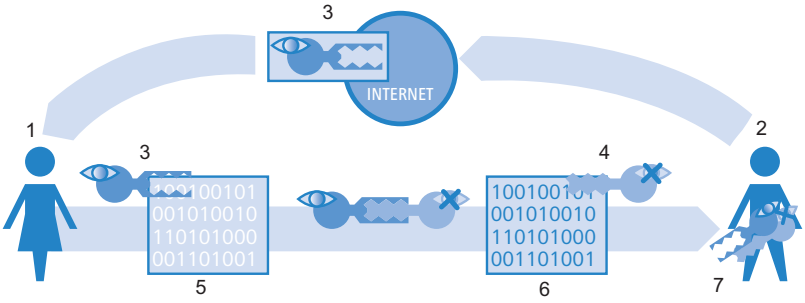


Figure 77: Asymmetrical encryption method

1: Alice
2: Bob
3: Bob's public key
4: Bob's private key
5: Encrypted message
6: Message in plain text
7: Bob's key pair, containing private and public key

- ☐ For secured communication, Bob first generates a key pair with a private key and public key that are uniquely matched. When generating these keys, Bob employs a procedure that makes it impossible to derive the private key from the public key. Bob can now distribute the public key without worries. He can e-mail it to Alice or simply store it on his web server.
- ☐ Alice now encrypts her message to Bob using his public key. Now Bob is the only one to decrypt this unreadable message with his private key. Even if unauthorized persons intercept the data on its way from Alice to Bob, no one but Bob can decrypt the plain text.

The asymmetrical encryption offers the following advantages over the symmetrical variant:

- A single key pair is required for each participant, and not for each communication relationship (as with synchronous encryption). With 1000 participants, every participant only requires his or her personal key pair, of which the public key is made publicly available. Instead of 500,000 secret keys, only 1000 key pairs are thus required with the public-key method.
- The unsecured transmission of the secret key to the communication partners is no longer necessary, as the public key is known on the other side of the communication relationship. This resolves an essential problem in the dynamic encryption of data between various participants.

Combination of Symmetrical and Asymmetrical Encryption

Asymmetrical encryption methods have quickly become established due to their security. However, security has its price: Asymmetrical encryption methods are slow. The mathematical procedures for encrypting and decrypting messages are much more complex than those of symmetrical encryption methods and therefore require more computing time. This is an exclusion criterion for the transmission of large data quantities.
The advantages of symmetrical and asymmetrical encryption can be enjoyed by suitably combining the methods. The secure asymmetrical encryption method is used to protect the transmission of the secret key. The connection's actual payload data is then encrypted using the quicker symmetrical encryption method.

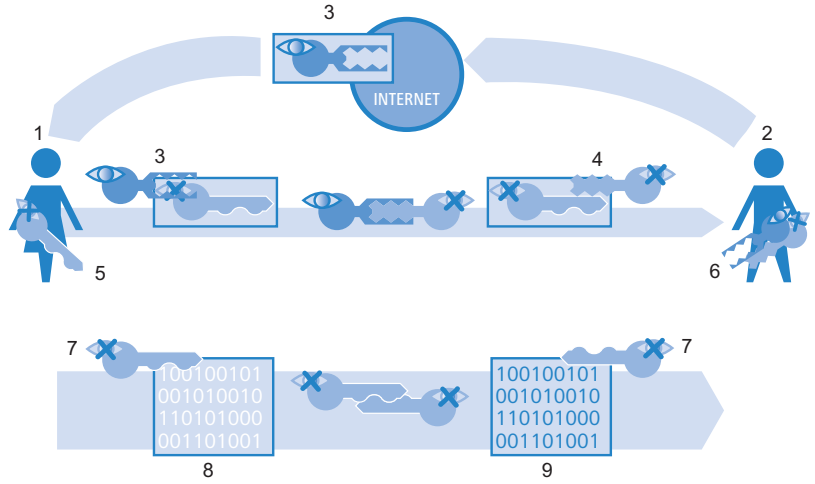


Figure 78: Combination of symmetrical and asymmetrical encryption

1: Alice
2: Bob
3: Bob's public key
4: Bob's private key
5: Alice's secret key
6: Bob's key pair, containing private and public key
7: Secret key
8: Encrypted message
9: Message in plain text

- ☐ In a first step, Bob creates his key pair and makes his public key publicly available.
- ☐ Alice uses the public key to encrypt a secret symmetrical key and sends it to Bob. This secret key is randomly generated for each transmission.
- ☐ Only Bob is able to decrypt the secret key with the aid of his private key.
- ☐ Alice and Bob then use the secret key for encrypting and decrypting the considerably larger payload data volumes.

Public Key Infrastructure

The combination of symmetric and asymmetric encryption methods make it possible to set up a secure data communication even via initially unsecured connections. Now we will shed some light on the aspect of authenticity: How does Alice know that the public key in use is actually from Bob? That is to say, the use of public keys depends on trust in the authenticity of the communication partner.
In order to secure this trust, publicly recognized credible offices confirm the key pairs of the asymmetric encoding that are being used In Germany, for example, the Federal Network Agency for Electricity, Gas, Telecommunications, Post and Railways is the highest credible authority for confirming digital keys. It in turn issues accreditations to suitable service providers who have likewise proved to be trustworthy.

Note: You can always find updated lists with accredited certification service providers, as well as references to revoked accreditations, on the website of the Federal Network Agency (www.bundesnetzagentur.de). A number of tax consultants and attorneys offices are included among the accredited service providers, for example.

The task of these authorities is to assign exactly one public key to one person or organization. This assignment is in a certificate and is publicly known. Therefore these providers are also called "certification authorities" or CA for short. The highest certification authority is considered the root/ master CA.
Bob turns to such a CA when he wants to have his public key certified for himself. To do this, he submits his public key to the CA, which confirms the association of the key with Bob.
The CA issues a certificate of this confirmation, which also contains data about Bob in addition to the public key, for example, his identity.

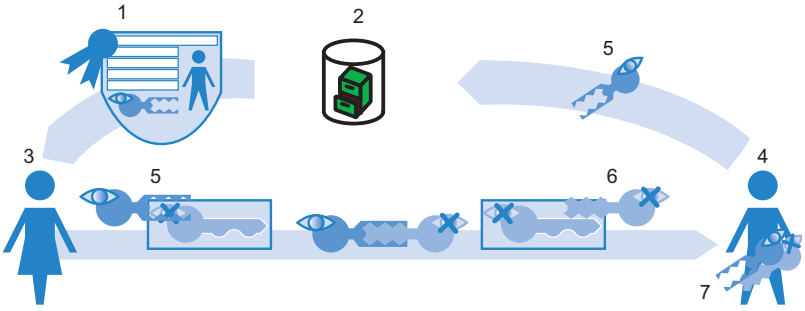


Figure 79: Method for issuing certificates for authorization

1: Certificate with public key from Bob, information on identity, signature of the CA
2: Certification authority (CA)
3: Alice
4: Bob
5: Bob's public key
6: Bob's private key
7: Bob's key pair with private and public key

The CA again signs the certificate, so that no one doubts the confirmation. Since the certificate consists only of a small amount of data, an asymmetric method is used for it. The asymmetric method operates in the opposite direction for the signature, however.

- The CA also has the key pair consisting of private and public key. As a trustworthy authority, its own key pair is considered reliable.
- The CIA calculates the hash value for the certificate, encrypts it and signs Bob's certificate with it. The CA therefore verifies the association of Bob's public key with his identity
  This process behaves in exactly the opposite manner as that for normal asymmetric encryption. Instead of protecting the data from unauthorized persons, encryption here has the purpose of confirming the CA's signature.
- With the public key of the CA, every participant in a data communication around the world is able to check the certificate signed with that key.
  Only the CA produces signatures with its private key, which it again encrypts with the CA's public key. This signature ensures that the certificate actually originates from the issuing CA.

6.5.2 Advantages of certificates

In some cases, the use of certificates for securing VPN connections is an alternative to the pre-shared key (PSK) method that is otherwise used.

- Secure VPN-client connections (with IKE main mode):
  When setting up PSK connections for peers with dynamic IP addresses, there is no possibility of using main mode. Instead of that, use aggressive mode with lower security. Using certificates enables usage of the main mode,and therefore an increase of security, even for peers with dynamic IP addresses.
- Higher security of the keys and passwords used:
  Pre-shared keys are just as susceptible as all other passwords. How the users handle these passwords ("human factor") thus has a considerable influence on the security of the connections. In a certificate-based VPN structure, the keys used in the certificates are automatically created with the desired key length. In addition, the random keys generated by computers, even with an identical key length, are more secure against attacks (e.g., dictionary attacks) than the pre-shared keys invented by human beings.
- Checking the authenticity of the counterparty is possible:
  In the VPN connection setup via certificates, it is necessary that the two opposing sides authenticate themselves. The certificates possibly contain additional information elements that help to check the remote terminals. The time limitation of certificates provides additional protection, e.g., for issuance to users who obtain temporary access to a network.
- Support of tokens and smart cards:
  Offloading the certificates onto external data media also allows them to be successfully integrated into "strong security" environments; reading passwords from computers or notebooks is out of the question.

The advantages of certificates contrast, however, with the higher expense for introducing and maintain a public key infrastructure (PKI).

6.5.3 Structure of certificates

- **Contents**

  In order to fulfill its tasks, a certificate contains a variety of information. Some parts of it are obligatory, others are optional. There are various formats in which a certificate is stored. A certificate according to the X.509 standard contains the following information, for example:

  - Version: This entry contains the version of the X.509 standard. The current version (06/2005) is "v3."
  - Serial number: An unambiguous serial number for identification of the certificate.
  - Signature algorithm: Identifies the algorithm with which the issuer signed the certificate. The digital signature of the issuer is also located there.
  - Validity: Certificates are valid for a limited period of time. Validity contains information on the duration.
  - Issuer: Data for identifying the issuer, e.g., name, e-mail address, nationality, etc.
  - Subject: Data for identifying the owner of the certificate, e.g., name, institution, e-mail address, nationality, city, etc.
  - Subject public key: Information as to the method that the issuer used in generating the public key of the certificate holder. The public key of the owner is likewise located in this item.

- **Target application**

  When creating the certificates, select the purpose for which the certificates are available. Some certificates are conceived specifically and only for web browsers and e-mail transmission, while others are generally usable for any purposes.

  Note: When creating the certificates, take care that you issue them for the desired purpose.

Formats

The ITU X.509 standard is a widely disseminated form for the certificates In a text representation, such a certificate resembles the following, for example:

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial number: 1 (0x1)
        Signature algorithm: md5WithRSAEncryption
      Issuer: CN=CA/Email=ca@trustme.dom, OU=Certificate Authority,
O=TrustMe Ltd, ST=Austria, L=Graz, C=XY,
        Validity:
            Not Before: Oct 29 17:39:10 2000 GMT
            Not After: Oct 29 17:39:10 2001 GMT
       Subject: CN=anywhere.com/Email=xyz@anywhere.com, OU=Web Lab,
O=Home, L=Vienna, ST=Austria, C=DE
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                    00:c4:40:4c:6e:14:1b:61:36:84:24:b2:61:c0:b5:
                    d7:e4:7a:a5:4b:94:ef:d9:5e:43:7f:c1:64:80:fd:
                    9f:50:41:6b:70:73:80:48:90:f3:58:bf:f0:4c:b9:
                    90:32:81:59:18:16:3f:19:f4:5f:11:68:36:85:f6:
                    1c:a9:af:fa:a9:a8:7b:44:85:79:b5:f1:20:d3:25:
                    7d:1c:de:68:15:0c:b6:bc:59:46:0a:d8:99:4e:07:
                    50:0a:5d:83:61:d4:db:c9:7d:c3:2e:eb:0a:8f:62:
                    8f:7e:00:e1:37:67:3f:36:d5:04:38:44:44:77:e9:
                    f0:b4:95:f5:f9:34:9f:f8:43
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Alternative Name:
                email:xyz@anywhere.com
            Netscape Comment:
                mod_ssl generated test server certificate
            Netscape Cert Type:
                SSL Server
    Signature algorithm: md5WithRSAEncryption
        12:ed:f7:b3:5e:a0:93:3f:a0:1d:60:cb:47:19:7d:15:59:9b:
        3b:2c:a8:a3:6a:03:43:d0:85:d3:86:86:2f:e3:aa:79:39:e7:
        82:20:ed:f4:11:85:a3:41:5e:5c:8d:36:a2:71:b6:6a:08:f9:
        cc:1e:da:c4:78:05:75:8f:9b:10:f0:15:f0:9e:67:a0:4e:a1:
        4d:3f:16:4c:9b:19:56:6a:f2:af:89:54:52:4a:06:34:42:0d:
        d5:40:25:6b:b0:c0:a2:03:18:cd:d1:07:20:b6:e5:c5:1e:21:
        44:e7:c5:09:d2:d5:94:9d:6c:13:07:2f:3b:7c:4c:64:90:bf:
        ff:8e
```

- **File types**
  Digital certificates and private keys have different file extensions, depending on the issuer. The following endings are typical, for example:
  - ☐ *.pfx and *.p12: PKCS#12 files
  - ☐ *.pem, *.cer and *.crt: BASE 64-coded certificates
  - ☐ *.cer, *.crt and *.der: DER-coded certificates
  - ☐ *.key: BASE64- or DER-coded keys
  - ☐ *.pvk: Microsoft-specific key format

  In the context of certificate-secured VPN connections, another file type is very important in addition to pure certificates: the PCKS#12 files, which may contain several components, including a certificate and private key among others. Processing the PCKS#12 files requires a password, which you define when exporting the certificates.

  Note: BASE64-coded certificates contain the following line in the header:
  `----- BEGIN CERTIFICATE -----`

- **Validity**
  A reference to a so-called certificate revocation list (CRL) is also optionally included. Certificates that have become invalid, for example, because an employee left the company and the company therefore withdrew his certificate, are listed in the CRLs. With this information, the proper CRL is used in checking the certificates.

6.5.4 Security

Observe the following safety aspects in handling certificates:

- ☐ Transmit the private keys only via secure connections, for example, HTTPS.
- ☐ Use sufficiently long and secure passphrases as keywords for the key or the PKCS#12 files.

6.5.5 Certificates in VPN connection setup

In addition to the fundamental information on the topic of certificates, we will consider the specific application for VPN connection setup in this section. For such a connection setup with certificate support, there must be certain information available on both sides of the connection:

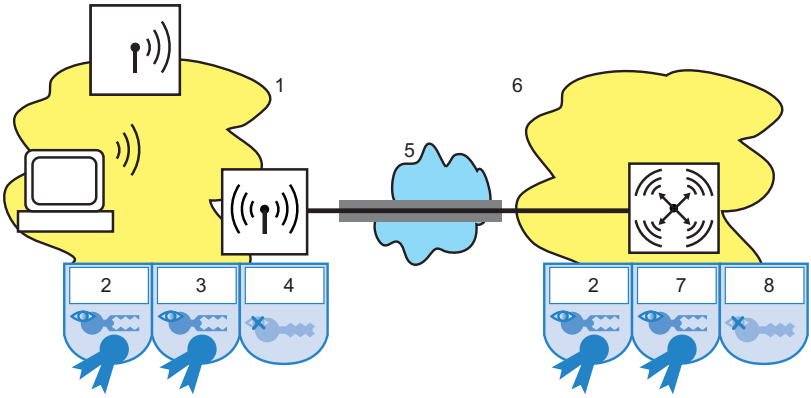


Figure 80: Usage of certificates for a VPN connection between headquarters and a branch office
1: Branch office
2: Root CA certificate
3: Branch office certificate

4: Branch office private key
5: Internet
6: Headquarters
7: Headquarters certificate
8: Headquarters private key

- The branch office has the following components:
  - Root CA certificate with the CA's public key
  - Its own device certificate with its own public key and the confirmation of identity. The checksum of the certificate is signed with the CA's private key.
  - Own private key
- The headquarters has the following components:
  - Root CA certificate with the CA's public key
  - Its own device certificate with its own public key and the confirmation of identity. The checksum of the certificate is signed with the CA's private key.
  - Own private key

The following processes, shown in main mode for simplicity, take place in the VPN connection setup (symmetrically in both directions):

- In a first packet exchange, the peers negotiate the encryption methods to be used in the authentication processes, for example. In this phase, both sides do not have any certain knowledge of whom they are currently negotiating with. That is insignificant up to this point, however.
- In the next step, the connected devices negotiate a shared key material for further use, containing symmetric keys and asymmetric key pairs, among others. In this state as well, both sides are still uncertain of whom they have negotiated the keys with.
- With the aid of the certificates, the device checks in the next step whether the peer from the negotiation of the key material is in fact the intended communication partner:
  - From the key material of the current negotiation, the branch office calculates a checksum (hash), which only the two involved peers (branch office and headquarters) calculate during this connection.
  - The branch office encrypts this hash with its own private key and thus creates a signature.
  - The branch office transmits the signature together with its own certificate to the peer in headquarters.

- Headquarters then checks the signature for the received certificate from the branch office. It does this with the aid of the public key in the root CA, which is available identically in both peers. If the peer at headquarters decrypts the signature from the branch office certificate created by the private key of the CA with the public key of the CA, then the signature is valid and the peer trusts the certificate.
- In the next step, headquarters then checks the signature of the encrypted checksum. It has already found that the branch office's public key from the corresponding certificate is valid in the previous step. Headquarters therefore checks whether it can decrypt the signed checksum with the branch office's public key. Headquarters calculates the same checksum from the key material of the current connection as did the branch office. If this check is successful, headquarters considers the peer "branch office" to be authenticated.

6.5.6 Certificates from certificate service providers

The certificates offered by public certification authorities are generally requested in different security classes. As security increases, the effort and expense for the applicant to authenticate its identity to the CA rises. Trustcenter AG in Hamburg uses the following classes, for example:

- Class 0: Trustcenter issues these certificates without checking the identity and uses them for test purposes for business clients.
- Class 1: In this level, Trustcenter checks the existence of an e-mail address. This level is suitable for private users who sign their e-mail, for example.
- Class 2: In this level as well there is no personal identity check. Transmitting an application with a copy of a commercial register entry, for example, is sufficient. This level is suitable for communication between companies that are known to one another.
- Class 3: In this level Trustcenter checks the person or company personally. Trustcenter checks the information in the issued certificates against a passport or an extract from the commercial registry. This level is suitable for advanced applications, for example, in e-business or online banking.

If you work together with a public certificate service provider, carefully check the security levels offered for the identity check. That way you can determine whether the certificates used actually meet your security needs.

6.5.7 Structure of one's own CA

Using public CAs is recommended for secure enterprise communication only to a certain extent:

- The issuance of new certificates is expensive and sometimes too slow.
- Public CAs transmit the keys that are used over poorly secured connections.
- Communication is based on trust of the CA.

Construction of a CA of one's own is therefore a suitable alternative for enterprise communication. The Microsoft CA on the Microsoft Windows 2003 Server, or OpenSSL as an open source version, are suitable for this. Create and manage all required certificates for securing data exchange yourself with a CA of your own, without dependency on outside authorities.

The use of a CA of their own is certainly more advisable to companies than using public providers for certification services. There are some important items already in the planning stage for the CA, however. Already when a Windows CA is installed, for example, the program establishes validity times for the root CAs that cannot be subsequently changed. Further aspects of planning include:

- The certificate policy, i.e., the security level which you seek with the aid of the certificates
- The namespace to be used
- The key lengths
- The lifetime of the certificates
- The management of blacklists

Precise planning pays off in every case, since later corrections can sometimes only be achieved at great expense.

6.5.8 Requesting a certificate with the standalone Windows CA

Note: A combination of a PKCS#12 file with a root certificate, a certificate of one's own devices and the public key of the device provide the best service for use in a device.

☐ Open the starting page of the Microsoft certificate service in your browser.
☐ Choose "Extended certificate request" as the certificate type.
☐ In the next step, choose the option "Create and submit a request to this certificate authority."

Note: Choose the option "BASE64" only if the root certificate is already present in a separate file.

☐ Enter the data for identification in the next step.

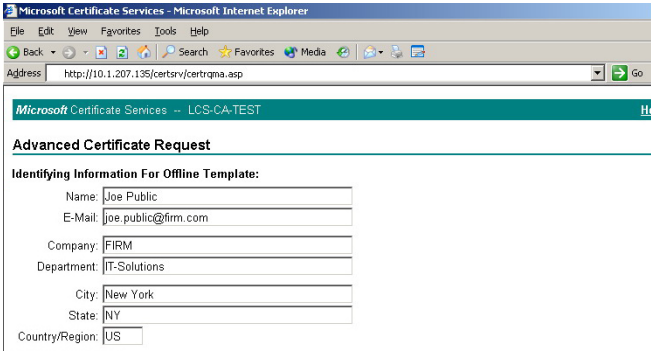


Figure 81: Request for extended certificate – entering data for identification

☐ In the same dialogue, select the option "Other ..." as the type of certificate and delete the value for "Object identifier" that then appears.

Figure 82: Extended certificate request – selecting the type of certificate

☐ Highlight "Automatic key generation." Thereby the CA automatically generates the public and private key for the current user.

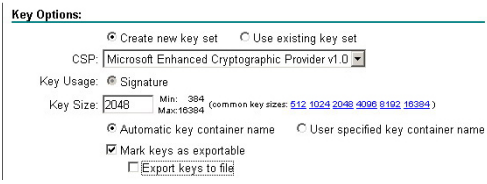


Figure 83: Extended certificate request – defining key options

☐ Select a suitable key length (matching the certificate policy). Activate the option for exportable keys.

Note: Since no export of the key is necessary at this point, you indeed not specify any filenames. While exporting, the program would create a file in the Microsoft-specific *.pvk format, which is worthless for further processing in a Hirschmann device.

☐ Finally choose the "SHA-1" algorithm and submit the certificate request by clicking the "Submit" button.

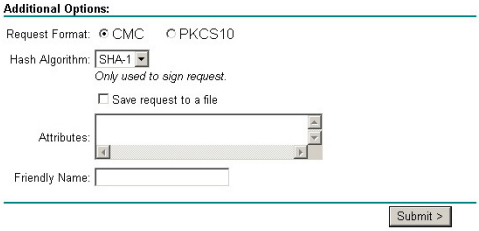


Figure 84: Extended certificate request – selecting hash algorithm

Note: You can view the status of the submitted certificate requests at any time via the homepage of the Windows CA. However you are only able to view the certificate requests from the same computer with which you submitted the request.

☐ Install the certificate on your computer as soon as the administrator of the CA has checked the certificate request and created the certificate

Note: You are only able to view the certificates from the same computer with which you submitted the request.

6.5.9 Exporting the certificate to a PKCS#12 file

When the certificate is installed, the device stores it in your operating system, but it does not yet exist as a separate file. You need one for installation in the Hirschmann device, however. To obtain a certificate in file form, it is necessary to first export it.

Export via the Windows console tree:

☐ To do this, open the management console with the MMC command at the prompt, and select the menu item File > Snap-in add/remove.

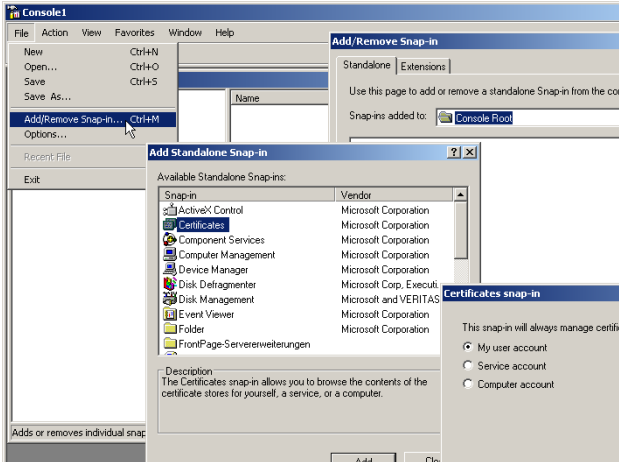


Figure 85: Adding certificates with Windows Management Console

☐ Click on Add.. and select the "Certificates" entry. Confirm with Add, then highlight "Own user account" and click on "Finish."

☐ In order to export the desired certificate into a file, click in the management console in the group Certificates – Current User > Own Certificates > Certificates with the right mouse button and select the entry All Tasks > Export in the context menu.

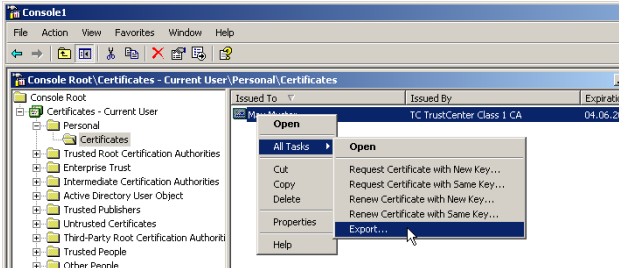


Figure 86: Exporting certificates with Windows Management Console

☐ In the process for the Certificate Export Wizard, activate the option for exporting the private key. Optionally delete the private key from the system after the export.

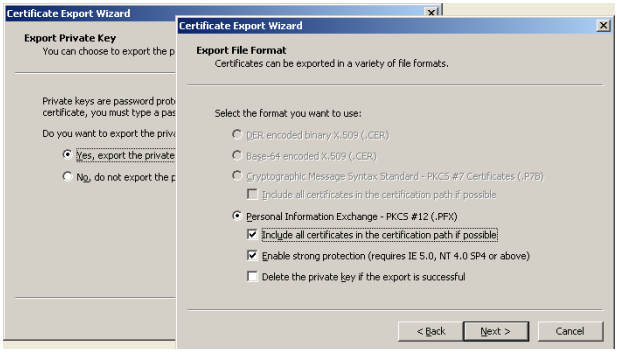

Certificate Export Wizard
Export Private Key
You can choose to export the p
Private keys are password prot
certificate, you must type a pas
Do you want to export the priv
Yes, export the private
No, do not export the p
Certificate Export Wizard
Export File Format
Certificates can be exported in a variety of file formats.
Select the format you want to use:
DER encoded binary X.509 (.CER)
Base-64 encoded X.509 (.CER)
Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
Include all certificates in the certification path if possible
Personal Information Exchange - PKCS #12 (.PFX)
Include all certificates in the certification path if possible
Enable strong protection (requires IE 5.0, NT 4.0 SP4 or above)
Delete the private key if the export is successful
< Back
Next >
Cancel

Figure 87: Certificate Export Wizard

Note: It is necessary to activate the option "Include all Certificates in the Certification Path." In this case, the program also exports the root certificate into the PKCS#12 file.

☐ During export the device prompts you to input a password for protecting the private key. Select a secure passphrase of sufficient length. You will again require this passphrase for the installation of the certificates in the Hirschmann device.

Note: Different environments also use the synonymous terms "password" or "PIN" for passphrase.

Export via the system controller

Alternatively you can open the certificates installed on the system via the system controller.

☐ To do this, select Start > System Controller > Internet Options and click the Certificates button on the "Contents" tab.

☐ Select the desired certificate and click on Export

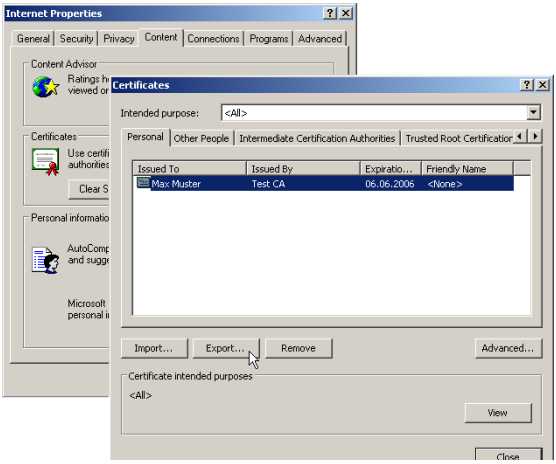


Figure 88: Exporting certificates via the system controller

Note: The subsequent Certificate Export Wizard behaves exactly as described in "Exporting certificates with Windows Management Console."

6.5.10 Creating certificates with OpenSSL

OpenSSL provides another possibility for creating certificates of your own and testing certificate connections. OpenSSL is available free as an open source project for Linux and Windows but as a command-line tool, it is less user-friendly than other CA versions.

Note: It is also necessary that you adapt the configuration file openssl.cnf to your specific needs. Further information can be found in the documentation for OpenSSL.

Installing OpenSSL

- ☐ Download a current version of OpenSSL from http://www.slproweb.com/products/Win32OpenSSL.
- ☐ Install the package and in the `./bin/PEM/demoCA` directory, also create the subdirectories:
  - `/certs`
  - `/newcerts`
  - `/cerl`.
- ☐ In the file openssl.cnf, change the path in the group [CA_default] to:
  `dir= ./PEM/demoCA`
- ☐ Start OpenSSL by double-clicking on openssl.exe in the `./bin` directory.

Issuing certificate for the root CA

- ☐ Create a key for the CA with the command:
  `genrsa -des3 -out ca.key 2048`

  Note: Note the passphrase that you input after the prompt for the CA key. You will need it again later.

  This command creates the file "ca.key" in the current directory.
- ☐ Create a certificate request for the CA with the command:
  `req -key ca.key -new -subj /CN=”Test_CA” -out ca.req`

  Note: Again input the passphrase for the CA key here.

  This command creates the file "ca.req" in the current directory.
- ☐ Create a certificate from the certificate request with the command:
  `x509 -req -in ca.req -signkey ca.key -days 365 -out ca.crt`
  This command signs the certificate request "ca.req" with the key "ca.key" and thus issues the certificate "ca.crt."

  Note: Again input the passphrase for the CA key here as well.

Issuing a certificate for users or devices

☐ Create a key for the device or the user with the command:
`genrsa -out device.key 2048`
This command creates the file "device.key" in the current directory.

☐ Create a certificate request for the device or the user with the command:
`req -key device.key -new -subj /CN=DEVICE -out device.req`
This command creates the file "device.req" in the current directory.

Note: In addition to this command, additional changes in the file "openssl.cnf" are necessary for definition of an extension.

☐ Create a certificate from the certificate request with the command:
`x509 -extfile openssl.cnf -req -in device.req -CAkey ca.key -CA ca.crt -CAcreateserial -days 90 -out device.crt`
This command signs the certificate request "device.req" with the key "ca.key" and thus issues the certificate "device.crt." The device also uses the configuration file openssl.cnf here.

☐ Export the certificate for the device or the user with the command:
`pkcs12 -export -inkey device.key -in device.crt -certfile ca.crt -out device.p12`
This command combines the key "device.key," the device certificate "device.crt," and the root certificate "ca.crt" and stores them jointly in the file "device.p12." Load this PKCS#12 file directly into the desired device.

6.5.11 Loading certificates into the Hirschmann device

It is necessary for the following components to be present in the Hirschmann device for the certificate-secured VPN connection setup:

- Root CA certificate with the CA's public key
- Its own device certificate with its own public key and the confirmation of identity. The checksum of the certificate is signed with the CA's private key.
- Own private key

If you have followed the instructions for issuing and exporting a certificate via a Windows CA, this information is now available in the form of a shared PKCS#12 file. Alternatively, you have used a different method and the individual components are present in separate files.

☐ Log onto the desired device with administrator rights via WEBconfig.
☐ Select the entry Upload Certificate or File.

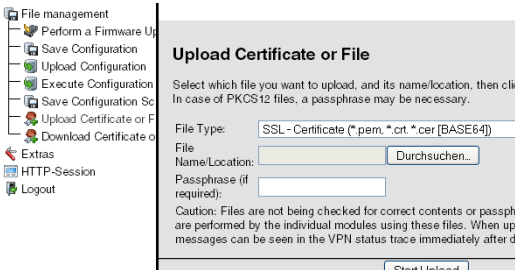


Figure 89: Load certificate into the Hirschmann device via WEBconfig.

☐ Select the components you will load into the device:
  ☐ Root certificate
  ☐ Device certificate
  ☐ Private key of the device
  ☐ PKCS#12 with a combination of root certificate, device certificate and private key

Note: Depending on the type of uploaded file, it may be necessary for you to input the respective passphrase.

You have the possibility of subsequently viewing the uploaded files in a list under HiLCOS Menu Tree > Status > File System > Content.

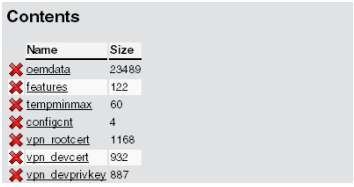


Figure 90: List of uploaded files in WEBconfig

Note: In the upload, the device breaks a combined PKCS#12 file down into the required parts automatically.

6.5.12 Backing up and uploading certificates with LANconfig

Use different certificates for decrypting defined services in a Hirschmann device. Load the certificates into the devices via LANconfig. You also have the possibility of reading out the certificates stored in a device via LANconfig and saving them in a file.

☐ Select the device into which you load a certificate or from which you back up a certificate.

☐ Click the selection with the right mouse button and select Configuration Management > Backup Certificate as File/Load Certificate as File in the context menu.

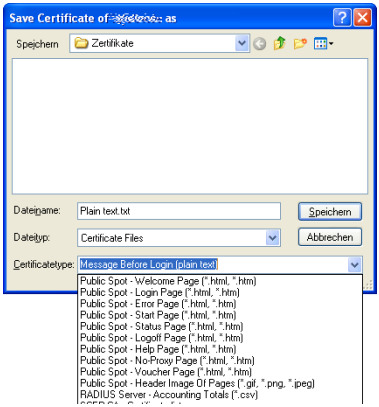

Save Certificate of as
Speichern
Zertifikate
Dateiname:
Plain text.txt
Speichern
Dateityp:
Certificate Files
Abbrechen
Certificatetype:
Message Before Login (plain text)
Public Spot - Welcome Page (*.html, *.htm)
Public Spot - Login Page (*.html, *.htm)
Public Spot - Error Page (*.html, *.htm)
Public Spot - Start Page (*.html, *.htm)
Public Spot - Status Page (*.html, *.htm)
Public Spot - Logoff Page (*.html, *.htm)
Public Spot - Help Page (*.html, *.htm)
Public Spot - No-Proxy Page (*.html, *.htm)
Public Spot - Voucher Page (*.html, *.htm)
Public Spot - Header Image Of Pages (*.gif, *.png, *.jpeg)
RADIUS Server - Accounting Totals (*.csv)

Figure 91: Saving or reading out certificates with LANconfig

☐ Select the storage location and type of the certificate that you are backing up or uploading and confirm the selection with Save/Open.

Note: By selecting several devices you upload a certificate file into several devices at the same time. Simultaneously backing up certificates from several devices is excluded, however. Depending on the type of certificate file, a passphrase may be necessary for uploading.

6.5.13 Adjusting VPN connections to certificate support

Note: The device sets up VPN connections with certificate support only if the Hirschmann device has the correct time of day. If the device has no up-to-date time of day, it also has no possibility of correctly assessing the validity of the certificates. The device then rejects the certificates and no connection is created.

Prepare different parts of the configuration in order to adjust VPN connections to support certificates:

- IKE proposals
- IKE proposal lists
- IKE keys
- VPN parameters
- Connection parameters

Note: Depending on the firmware status, your device already contains some of the required values. In this case, simply check the values for correct settings.

Note: If you are converting a remote device to certificate support via VPN, then by all means convert the remote device first. Do this before you change the connection of the local device. Otherwise, if you change the local configuration you cannot set up a connection to the remote device.

☐ Two new proposals with the exact designations "RSA-AES-MD5" and "RSA-AES-SHA" appear in the lists of proposals. They both use "AES-CBC" as their encryption and the "RSA signature" authentication mode, and differ only in their hash method (MD5 or SHA1)

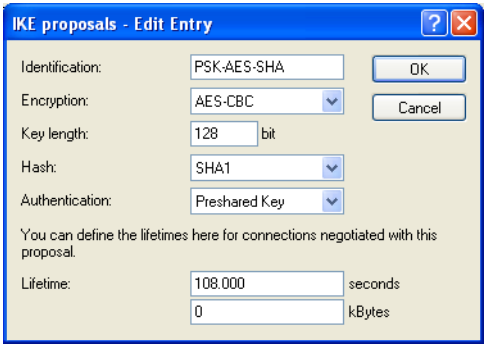


Figure 92: Entries into the IKE proposals

LANconfig: VPN > IKE-Param. > IKE proposals
WEBconfig: HiLCOS Menu Tree > Setup > VPN > Proposals > IKE

☐ A new list with the exact designation "IKE_RSA_SIG," which contains the two new proposals "RSA-AES-MD5" and "RSA-AES-SHA," is required in the proposal lists.

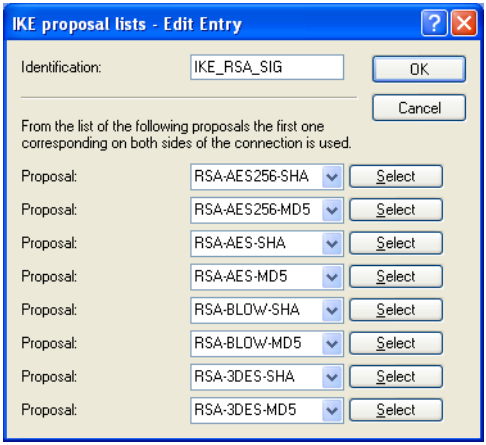


Figure 93: New list in the IKE proposals

LANconfig: VPN > IKE-Param. > IKE Proposal Lists
WEBconfig: HiLCOS Menu Tree > Setup > VPN > Proposals > IKE Proposal Lists

☐ Insert the appropriate identities in the list of IKE keys for all certificate connections.

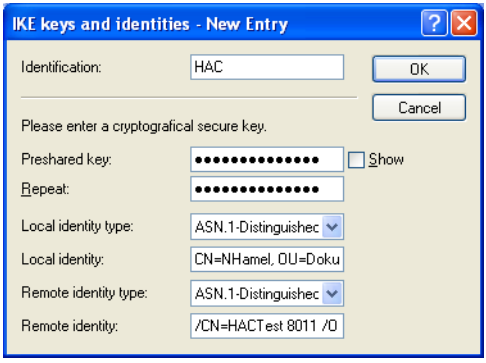


Figure 94: IKE keys in LANconfig

LANconfig: VPN > IKE Auth. > IKE keys and identities

- Delete the pre-shared key when it finally has no more use.
- Adjust the type of the identities to "ASN.1 Distinguished Names" (local and remote).
- Enter the identities exactly as in the certificates. Separate the individual values for "CN," "O" or "OU" by commas or slashes.
  It is required that you list all the values entered in the certificates in the same order. Check the contents of the certificates via the system controller if necessary. To do this, select Start > System Controller > Internet Options and click the Certificates button on the "Contents" tab. Open the desired certificate and select the appropriate value on the "Details" tab. Here you will find the required ASN.1 Distinguished Names with the associated abbreviations for the requester, for example.. Enter the values in the certificates from top to bottom into the IKE key from left to right. Please note the case-sensitivity here.

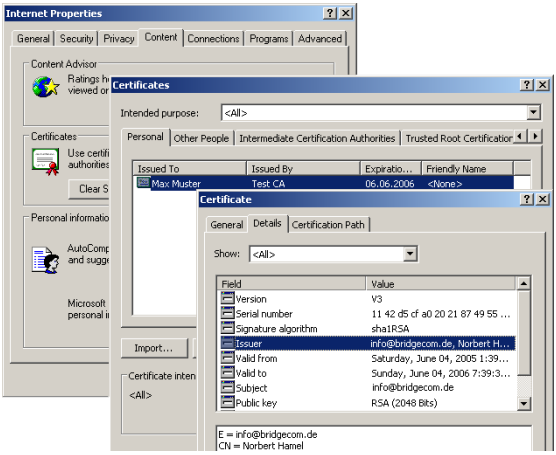


Figure 95: Certificates in the Internet options

Note: The display of certificates under Microsoft Windows shows older abbreviated forms for some values. These include, for example, "S" in place of "ST" for "stateOrProvinceName" or "G" in place of "GN" for "givenName." For these, use only the current abbreviated forms "ST" and "GN."

Note: You can enter special characters in the ASN.1 Distinguished Names by inputting the ASCII code in hexadecimal representation with a preceding backslash. For example, "\61" corresponds to a lowercase "a."

You can find the IKE key under WEBconfig or Telnet at the following places:

Configuration tool	Call
WEBconfig	HiLCOS Menu Tree > Setup > VPN > Certificate Keys > IKE Keys
Terminal/Telnet	/Setup/VPN/Certificate keys/IKE keys

☐ In the IKE connection parameters, place the default IKE proposal lists for incoming aggressive mode and main mode connections on the proposal list "IKE_RSA_SIG." Also note the setting of the default IKE group, the adjustment of which may be required by the next step.
The default IKE proposal lists and default IKE groups are found under LANconfig in the "VPN" configuration area on the "Defaults" tab.

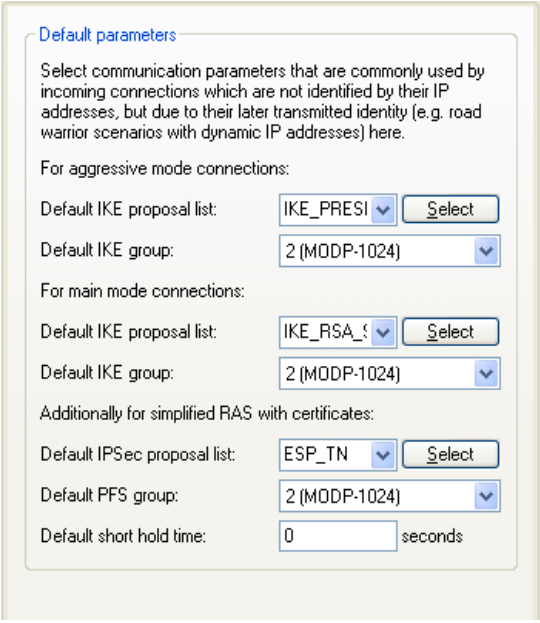


Figure 96: Editing IKE connection parameters

You can find the IKE proposal lists and the default IKE groups under WEBconfig or Telnet at the following places:

Configuration tool	Call
WEBconfig	HiLCOS Menu tree > Setup > VPN
Terminal/Telnet	/Setup/VPN

☐ Finally adjust the VPN connections in the APN connection parameters to the use of the correct IKE proposals ("'IKE_RSA_SIG"). It is necessary that the values for "PFS group" and "IKE group" match the values set in the IKE correction parameters.
The VPN correction parameters are found under LANconfig in the "VPN" configuration area on the tab "General" with a click on the Connection Parameters button.

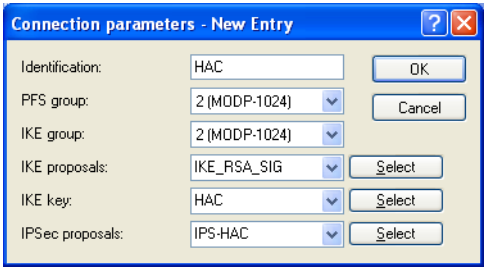


Figure 97: Checking the connection parameters in LANconfig

You can find the VPN connection parameters under WEBconfig or Telnet at the following places:

Configuration tool	Call
WEBconfig	HiLCOS Menu tree > Setup > VPN > VPN Layer
Terminal/Telnet	/Setup/VPN/VPN-Layer

6.5.14 Creating certificate-based VPN connections for LAN coupling using the Setup Wizard

With the Setup Wizard from LANconfig you have the possibility of setting up LAN couplings via VPN quickly and conveniently.

Note: Setting up VPN connections with certificate support is possible only if the Hirschmann device has the correct time of day and you have loaded the appropriate certificates into the device.

- ☐ Select the Wizard for connecting networks via VPN. Then select the VPN connection authentication via certificates (RSA signature) in the appropriate dialog.
- ☐ Enter the identities from the local and remote device certificate. Transfer the complete data from the respective certificates in the correct order: Enter the ASN.1 Distinguished Names listed under Windows in the certificates from top to bottom into LANconfig from left to right.

Note: The display of certificates under Microsoft Windows shows older abbreviated forms for some values. These include, for example, "S" in place of "ST" for "stateOrProvinceName" or "G" in place of "GN" for "givenName." For these, use only the current abbreviated forms "ST" and "GN."

Note: The Telnet command `show vpn cert` shows the contents of the device certificate in a Hirschmann device, including the input relative distinguished names (RDN) under "subject."

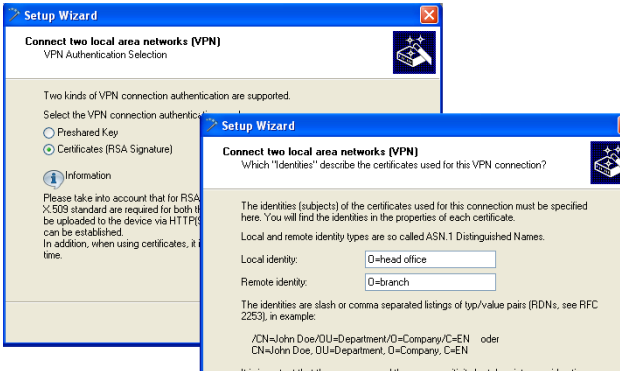

Setup Wizard
Connect two local area networks (VPN)
VPN Authentication Selection
Two kinds of VPN connection authentication are supported.
Preshared Key
Certificates (RSA Signature)
Information
Setup Wizard
Connect two local area networks (VPN)
Which "Identities" describe the certificates used for this VPN connection?
The identities (subjects) of the certificates used for this connection must be specified here. You will find the identities in the properties of each certificate.
Local and remote identity types are so called ASN.1 Distinguished Names.
Local identity:
O=head office
Remote identity:
O=branch
The identities are slash or comma separated listings of typ/value pairs (RDNs, see RFC 2253), in example:
/CN=John Doe/OU=Department/O=Company/C=EN oder
CN=John Doe, OU=Department, O=Company, C=EN

Figure 98: Setup Wizard for LAN-LAN coupling

☐ Select the optimized connection setup with IKE and PFS group 2 if possible. Select group 5 for IKE and PFS only if the remote terminal demands it.

☐ Enter the names of the VPN remote terminal, the IP address and the network mask of the remote network as well as a domain for the DNS relay, if appropriate. Activate the "Extranet" function and "netBIOS Routing" as needed.

6.5.15 Simplified network connection with certificates – pro-adaptive VPN

For VPN-coupling of large network structures, it is advantageous if the configuration effort for the setup of the new subnetwork is limited to the VPN router there and the configuration of the central dial-in router remains untouched. In order to achieve this simplified network connection, the devices dialing in transfer their identity with the aid of a certificate.

If you have activated the simplified dial-in with certificates for the Hirschmann router in the central station, then the remote routers themselves specify a network during the IKE negotiation in Phase 2. The routers then use it for the connection. This network is used, for example, when setting up the VPN connection in the remote router. The Hirschmann router in the central station accepts the opposed network if you have activated the option "Allow remote terminal selection of the remote network." It is also necessary that the parameters used by the client in the dial-in match the default values of the VPN router.

Note: In the configuration of the remote terminals that dial in, see to it that each remote terminal requests a special network. In that way there will be no conflicts between the network addresses.

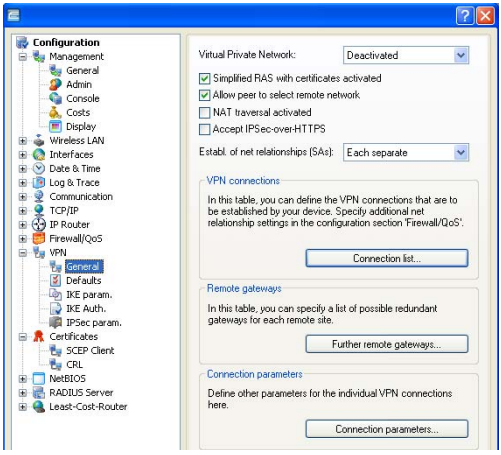


Figure 99: Simplified network connection with certificates

Configuration tool	Call
LANconfig	VPN/General and VPN > General > Defaults
WEBconfig, Telnet	HiLCOS Menu tree > Setup > VPN

Note: By activating the simplified certificate dial-in, all remote routers have the possibility of dialing in to the respective network with a valid certificate that bears the signature of the issuer of the root certificate located in the device. The router does not need any further configuration. You present undesired dialing-in exclusively by blocking certificates and using a certificate revocation list (CRL).
Simplified connection of networks with certificates is therefore limited to Hirschmann routers that support CRL.

6.5.16 Requesting certificates by means of CERTREQ

Some VPN gateways expect that the remote terminal will request certificates to be transmitted via a "certificate request" (CERTREQ) in an IPSec mediation authenticated by means of an RSA signature. Among other things, this allows a selection of the certificate to be used, as long as the gateway trusts multiple CAs.
In order to allow the setup for such VPN gateways, Hirschmann routers send a corresponding CERTREQ during the connection setup. It contains the issuer of the root certificate stored in the Hirschmann router.

6.5.17 Certificate revocation list - CRL

Certificates for VPN connections contained a validity period in the form of starting and ending dates. Set up a VPN connection during this time via this certificate. If an employee who uses such a certificate for mobile VPN access, for example, leaves the company, it may be desirable to prematurely declare the certificate invalid. This is done so that there is no longer a possibility for access to the company network even with an unchanged configuration of the VPN routers.

Since the certificate itself is with the employee, and the latter cannot make any changes to the certificate, the device uses a certificate blocking list. The invalid certificates are entered in such a certificate blocking list, which is supported by Microsoft CA or OpenSSL, for instance. The CRL is available on a suitable server. The VPN router itself enters the URL from which a router loads the CRL into its memory into the root certificate and/or its configuration. This CA updates the CRL regularly, so that VPN routers promptly recognize changes in the CRL due to withdrawn certificates. When the CA is imposed, there is usually a time span after which the CRL is regularly updated. After the update of the CRL and the storage of the CRL on the server (manually or automatically) the VPN router updates this new information. To do this, the router reads out the validity period of the CRL and attempts to load the current CRL shortly before expiration. Alternatively you find a regular update – independently of the validity period of the CRL – in a Hirschmann router. In the connection setup, the VPN router checks whether the current CRL contains a certificate of the remote terminal. In that way, the device refuses connections to remote terminals with invalid certificates.

- **Configuration of the CRL function**
  In addition to the path of the CRL, specify additional parameters such as the update interval for the configuration of the CRL function.

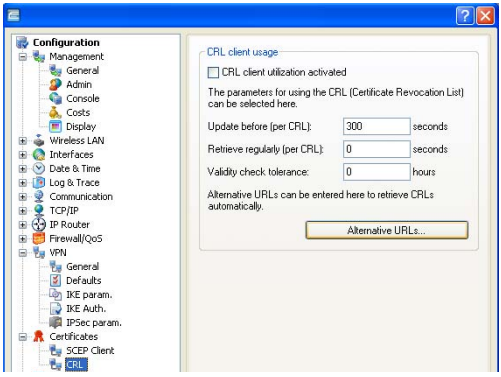


Figure 100:Configuration of the CRL function

Configuration tool	Call
LANconfig	Certificates > CRL client
WEBconfig, Telnet	HiLCOS Menu tree > Setup > Certificates > CRLs

- CRL functionality [default: off]
  Activated: When checking a certificate, the device also consults the CRL (if available).

  Note: If you have activated this option and the device does not find a valid CRL because, for example, there is no connection to the server, then the router refuses all connections and interrupts existing connections.

- Retrieval before expiration [default: 300 seconds]
  The point in time before expiration of the CRL from which the device attempts to load a new CRL. This value is increased by adding a random component in order to avoid excessively many requests to the server. When this point in time is reached, a regular update that may be activated stops.

  Note: If the loading of the CRL is unsuccessful in the first attempt, then the device starts new attempts in short intervals of time.

- Retrieval regular [default: 0 seconds]
  The length of the period of time after which the device periodically attempts to obtain a new CRL. With this, you can download CRLs published out of sequence early. With an entry of "0" you deactivate the regular retrieval.

  Note: If loading of the CRL is unsuccessful for regular updates, then the device will not start any attempts until the next regular date.

- Validity tolerance
  The device allows certificate-based connections even after the expiration of the CRL validity within the period of time entered here. With this tolerance time, you can prevent the device from refusing or disconnecting conditions in case of a short-term interruption of connection to the CRL server.

Note: Within the period of time set here, you can keep a connection in existence or set up a new connection with the aid of the certificates already blocked in the CRL.

- Alternative URLs
  The certificates usually contain the address from which the device retrieves a certificate revocation list (CRL) as crlDistributionPoint. Specify alternative URLs in this table. After system startup, the device loads the corresponding CRLs automatically from these URLs and uses them in addition to the lists specified in the certificates.

Display of the CRL status in LANmonitor

Information on the validity period and the publisher of the current CRL in the Hirschmann router can be found in LANmonitor.

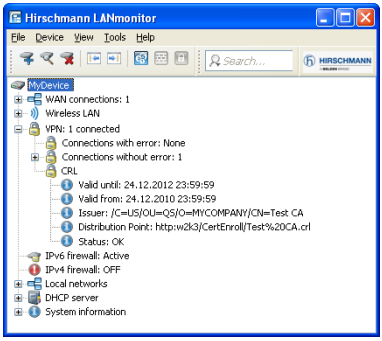


Figure 101:CRL status in LANmonitor

6.5.18 Diagnosis of the VPN certificate connections

The following commands at the console provide helpful information in case the device has no possibility of setting up a functional connection:

- `trace + vpn-status`
  Shows a trace of the current VPN connections.
- `show vpn long`
  Shows the contents of the VPN configuration, among other things, the distinguished names (DN) that are registered.
- `show vpn ca`
  Shows the content of the root certificate.
- `show vpn cert`
  Shows the content of the device's own certificate.

6.6 Multilevel certificates for SSL/TLS

6.6.1 Introduction

For large or spatially distributed organizations, multilevel certificate hierarchies are used, in which one or more intermediate CAs issue final certificates. The intermediate CAs are themselves certified by a root CA.

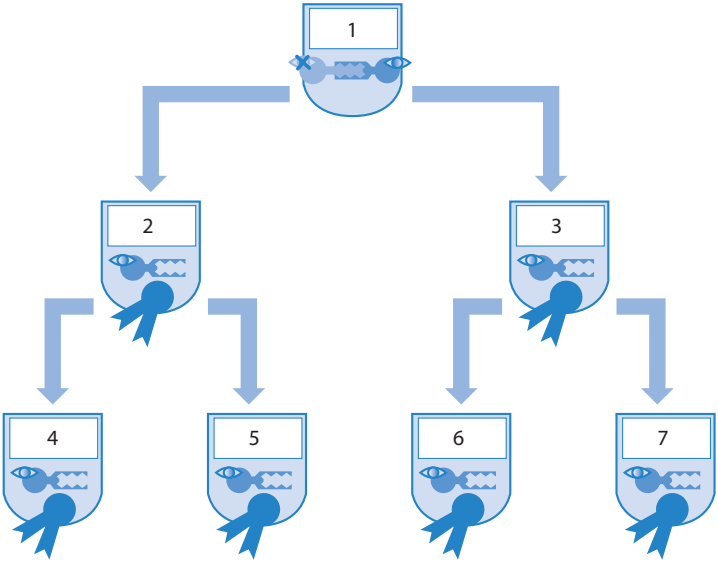


Figure 102:Multilevel certificates for SSL/TLS

1: Root CA
2: CA Europe
3: CA America
4: User 01
5: User 02
6: User 03
7: User 04

Checking the entire certificate hierarchy is necessary for authenticating the final certificates.

6.6.2 SSL/TLS with multilevel certificates

Applications that are based on SSL/TLS, (e.g. EAP/802.1x, HTTPS or RADSEC) load the SSL (server) certificate, together with its private key and the CA certificate(s) of the intermediate levels, as PKCS#12 containers into the device.
The remote terminals then send only their own device certificate to the device during connection setup. The Hirschmann router checks the certificate chain for validity.

6.6.3 VPN with multilevel certificates

To set up certificate-based VPN connections, the device stores a private key, a device certificate and the certificate of the CA in the file system. Use either the individual files or a PKCS#12 file for single-layer certificate solutions. After uploading and the input of the passphrase, the router breaks such a container down into the three above-mentioned components.
For a multilevel certificate hierarchy, however, the device uses a PKCS#12 container with the certificates of the CAs of all levels in the certificate chain. After uploading and the input of the passphrase, the device unpacks the certificate of the next CA "above" the device, in addition to the private key and the device certificate. The remaining certificates remain in the PKCS#12 container. For updating the VPN configuration, the router reads the unpacked certificates and the certificates from the container. When setting up a VPN connection, the remote terminal then transmits only its own device certificate. The device then checks the certificate against the existing hierarchy.

Note: It is necessary for the certificate structures to match for both remote terminals. That means that the hierarchy of the requesting VPN device requires only certificates that likewise occur in the hierarchy of the other VPN device.

6.7 Certificate enrollment via SCEP

To secure communication over publicly accessible networks, certificate-based VPN connections are being used more and more. The high-security demand of the digital certificates is countered by a considerable extra expense for managing and distributing the certificates. This expense primarily arises in the branch offices or home offices of a distributed network structure.
In order to set up a certificate-based VPN connection from a remote terminal to the network of a central system, a Hirschmann VPN router requires the following components:

- ☐ Certificate of the root CA with the public key of the CA. It is necessary that a certificate issued by the same CA likewise be present in the central station.
- ☐ Device's own certificate with its own public key. This certificate contains the signature with the private key of the CA and creates the confirmation of identity.
- ☐ Its own private key.

Note: The SCEP client supports one certificate for each purpose of use (VPN, WLAN controller). For the CAs, you have the opportunities to select the setting "general" in addition to the concrete purpose of use. If you enter a general CA then the router uses this CA for all certificates.

For a conventional structure of the VPN with certificates, it is necessary to enter the keys and certificates manually into the individual devices and change them promptly before expiration. The Simple Certificate Enrollment Protocol (SCEP) permits secure and automated distribution of certificates via an appropriate server. This reduces the expense for the rollout and the maintenance of certificate-based network structures. The router itself

generates the key pair for the device directly. The private part of the key thus never leaves the device, which represents a considerable increase in security. A Hirschmann VPN router has the possibility of calling up both the root certificate of the CA and its own device certificate via SCEP automatically from a central location.

6.7.1 SCEP server and SCEP client

An SCEP server takes over the provision and maintenance of the certificates. In addition to the function of an ordinary certification authority (CA) the server also has the SCEP functionality. Implement this server, e.g., as a Windows 2000 Server CA with a special plug-in (mscep.dll). There are also a number of CA solutions that support SCEP, for example the open-source solution OpenCA (www.openca.org).
The SCEP extension, i.e. mscep.dll, creates an additional instance on the server that processes the SCEP clients and hands them over to the actual CA. This instance is known as a registration authority (RA).
The VPN devices, (that is, the Hirschmann VPN routers) appear as SCEP clients, which automatically retrieve the required certificates from the central server. The device also requires the certificates signed by the CA from the RA (registration authority) for the SCEP process. For the actual VPN operation, the Hirschmann VPN routers primarily require valid system certificates (device certificates). The other certificates that are used are necessary solely for the SCEP process.

6.7.2 The process sequence of a certificate distribution

In overview, the distribution of certificates via SCEP runs according to the following diagram:

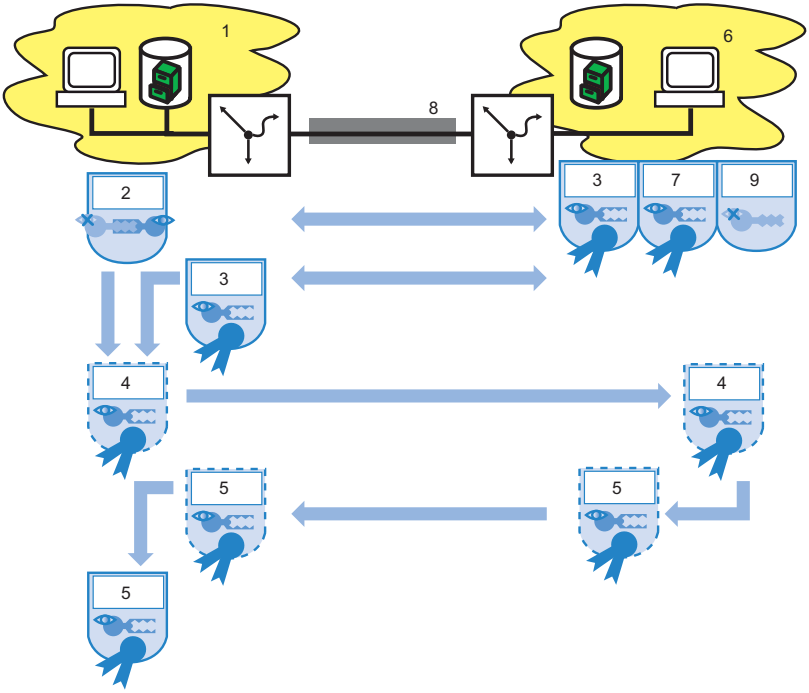


Figure 103:Process sequence of the certificate distribution

1: Branch office
2: Branch office key pair
3: Root CA certificate
4: Certificate request

5: Device certificate
6: Headquarters
7: Headquarters certificate
8: Internet
9: Headquarters private key

- Generating key pair in the Hirschmann VPN router:
  You have the possibility to generate a key pair in the Hirschmann VPN router. The device later transmits the public part of this key pair together with the request to the SCEP server. The private part of the key pair remains in the SCEP client (Hirschmann VPN router). The fact that the private key never leaves the device at any time represents an increase in security compared to manual certificate distribution, for example via PKCS#12 containers.
- Retrieving CA and RA certificates:
  In order to communicate with RA/CA, the relevant RA and CA certificates are necessary in the Hirschmann VPN router. In a retrieval of the CA certificate via SCEP, the router automatically checks the fingerprint configured in advance as to whether the retrieved certificates actually originate from the desired CA. SCEP itself does not offer a mechanism for automatic authentication of the CA certificates on the SCEP client side. If the administrator of the Hirschmann VPN router has no access to the CA himself, then he can check the fingerprint by telephone with the CA admin, for example.
- Creating and encrypting a request for a device certificate
  The SCEP client gathers the configured information for the request for a system or device certificate. These include the identity of the requesting device (requester), the "challenge phrase" and the passphrase for the automatic processing of the request on the SCEP server. This request bears the signature of the private part of the key pair.
- Transmitting request to the SCEP server:
  The SCEP client subsequently transmits the request together with its public key to the SCEP server.

- Checking the certificate request on the SCEP server and issuance of the device certificate:
  The SCEP server decrypts the received request and then issues a system or device certificate for the requester. SCEP distinguishes the following methods for processing the requests:
  - Ensure the authenticity of the requester in the automatic processing via the challenge phrase. Mscep.dll creates the challenge phrase automatically on a Windows CA server. The CA is valid for one hour. If the challenge phrase in the certificate request coincides with the currently valid value on the server, then the device automatically issues the system certificate.
  - In the manual case, the SCEP server puts the certificate request into a wait state until the acceptance or denial of the CA administrator is certain. During this waiting time, the SCEP client regularly checks whether the SCEP server has issued the required system certificate in the meantime.
  - With RA-AutoApprove the device identifies the client via a certificate validly issued by the CA.
- Retrieving the device certificate from the SCEP server:
  As soon as the certificate is ready, the client determines by regular polling that it is possible to retrieve the certificate.
- Checking device certificate and providing it for VPN operation

6.7.3 Configuration of SCEP

For configuration of SCEP, define global parameters for the SCEP operation and the CAs from which the device retrieves the certificates.

Note: In addition to the configuration of the SCEP parameter, an adjustment of the VPN configurations may be necessary.

Configuration tool	Call
WEBconfig, Telnet	HiLCOS Menu tree > Setup > Certificates > SCEP Client

Global SCEP parameters

- Active:
  Turns the usage of SCEP on or off.
  Possible values: Yes, No
  Default: No
- Repeat-after-error interval:
  The interval in sections for repetitions after any type of error.
  Default: 22
- Check-pending-request interval
  Interval in seconds for checking pending certificate request.
  Default: 101
- Update system certificates before process:
  Lead time in days for timely request of new system certificates (device certificates).
  Default: 2
- Update CA certificates before process:
  Lead time in days for timely retrieval of new RA/CA certificate.
  Default: 1

- Actions
  - Reinit:
    Starts the manual re-initialization of the SCEP parameters. As in ordinary SCEP initialization, the device retrieves the necessary RA and CA certificates from the CA and stores them in the file system of the Hirschmann VPN router in such a manner that usage in VPN operation is not yet possible.
    - If the available system certificate matches the retrieved CA certificate, the router uses the system certificate, the CA certificate and the private device key for the VPN operation.
    - If the existing system certificates do not match the retrieved CA certificate, a new certificate request to the SCEP server is first required. The router can use the system certificate, the CA certificate and the private device key for VPN operation only if the device has issued and retrieved a new system certificate matching the CA certificate.
  - Updating:
    Manually starts the request for a new system certificate independently of the remaining period of validity. The device generates a new key pair.
  - Cleaning SCEP file system:
    Starts the cleaning of the SCEP file system.
    - Deleted: RA certificates, pending certificate requests, new and inactive CA certificates, new and inactive private keys.
    - Retained: system certificates currently used in the VPN operation, private keys for them and the CA certificates currently used in the VPN operation.

- Configuration of the CAs
  - Name:
    configuration name of the CA
  - URL
    URL of the CA.
  - DN:
    Distinguished Name of the device. Firstly, CAs are associated with system certificates (and conversely) via this parameter. Secondly, this parameter also plays a part in assessing whether received or existing certificates correspond to the configuration.

- Enc-Alg:
  The device encrypts the payload of the certificate request with this algorithm.
  Possible values: DES, 3-DES, Blowfish
  Default: DES
- Identifier:
  CA identifier. Some Web servers require this to assign the CA.
- RA-Autoapprove:
  Some CAs offer the possibility of using a certificate already issued by this CA as verification of the authenticity for subsequent requests. You determine with this option whether the device signs new requests with the existing system certificate if a system certificate already exists.
  Possible values: Yes, No
  Default: No
- CA signature algorithm
  The router signs the certificate request with this algorithm.
  Possible values: MD5, SHA1
  Default: MD5
- CA fingerprint algorithm:
  Algorithm for signing the fingerprint. Determines whether the device undertakes a check of the CA certificates based on the fingerprint, and with what algorithm. It is necessary that the CA fingerprint agrees with the checksum that results when the algorithm is used.
  Possible values: Off, MD5, SHA1
  Default: Off
- CA fingerprint:
  Based on the checksum (fingerprint) registered here, you check the authenticity of the obtained CA certificate (according to the set CA fingerprint algorithm).
- Usage:
  Indicates the purpose of use of the registered CA. The device retrieves the CA registered here solely for the corresponding purpose of use.
  Possible values: VPN, WLAN controller, general
  Special values: General If a general CA is present, an additional one cannot be configured, because otherwise the choice of the CA is unclear.

- Configuration of the system certificates
  - Name:
    Configuration name of the certificate
  - CADN:
    Distinguished Name of the CA. Firstly, CAs are associated with system certificates (and conversely) via this parameter. Secondly, this parameter also plays a part in assessing whether received or existing certificates correspond to the configuration.
  - Subject:
    Distinguished Name of the subject of the requester.
  - ChallengePwd:
    Passphrase for the automatic issuance of the device certificates on the SCEP server.
  - SubjectAltName:
    Further information on the requester, e.g., domain or IP address.
  - KeyUsage:
    Arbitrary, comma-delimited combination of:
    - digitalSignature
    - nonRepudiation
    - keyEncipherment
    - dataEncipherment
    - keyAgreement
    - keyCertSign
    - cRLSign
    - encipherOnly
    - decipherOnly
    - critical (possible, but not a recommendation)
  - extended Key Usage:
    Arbitrary, comma-delimited combination of:
    - critical
    - serverAuth
    - clientAuth
    - codeSigning
    - emailProtection
    - timeStamping
    - msCodeInd
    - msCodeCom
    - msCTLSign
    - msSGC
    - msEFS
    - nsSGC

- 1.3.6.1.5.5.7.3.18 for WLAN controller
- 1.3.6.1.5.5.7.3.19 for access points in managed mode

- System certificate key length.
  Length of the key that the device generates for itself.
  Possible values: 31 or greater
- Usage:
  Indicates the purpose of use of the registered certificates. The device retrieves the certificates registered here solely for the corresponding purpose of use.
  Possible values: VPN, WLAN controller

6.8 Extended Authentication Protocol (XAUTH)

6.8.1 Introduction

When remote terminals dial in via WAN connections (e.g., via PPP) RADIUS servers are often used to authenticate the users. Over time the more secure (encrypted) and inexpensive VPN connections displaced the previously customary WAN connections. Setting up VPN connections via IPSec with IKE, however, does not allow one-directional authentication of users via RADIUS or the like.
The Extended Authentication Protocol (XAUTH) offers the possibility of expanding the authentication in negotiating IPSec connections with an additional level. This is used for authenticating the user data. For this purpose, the device carries out an additional authentication with XAUTH username and XAUTH password, protected by the previously negotiated encryption, between the first and second IKE negotiation phase. This authentication uses a RADIUS server and thus allows continued use of RADIUS databases in the migration to VPN connections for dial-in clients. The authentication alternatively uses an internal user table in the device.

Note: In order to design the use of XAUTH to be particularly secure, use dial-in via RSA-SIG (certificates) in place of the pre-shared key method (PSK) if possible. Ensure that the VPN gateway accesses only the certificate of the respective correct remote terminal and not all certificates issued by the same CA.

6.8.2 XAUTH in HiLCOS

In the Hirschmann router, the XAUTH protocol uses the entries in the PPP table to authenticate the remote terminal. The use of entries in the PPP table is dependent on the direction of the connection setup, i.e., the XAUTH operating mode:

XAUTH operating mode	Server	Client
XAUTH user name	Remote terminal from the PPP table Here the device uses the entry from the PPP table in which the PPP remote terminal corresponds to the transmitted XAUTH username. The PPP remote terminal is also required to correspond to the VPN remote terminal in use.	Username from the PPP table Here the device selects the entry from the PPP table in which the PPP remote terminal corresponds to the VPN remote terminal in use.
XAUTH passphrase	Passphrase from the PPP table	Passphrase from the PPP table

6.8.3 Configuration of XAUTH

Use the XAUTH protocol separately for each VPN remote terminal Only define the XAUTH operating mode.

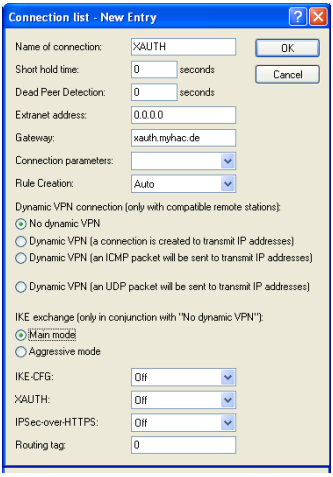


Figure 104:New entry in the connection list

LANconfig: VPN > General > Connection List

WEBconfig: Setup > VPN > VPN Remote Terminal

- XAUTH:
  Activates the use of XAUTH for the selected VPN remote terminal.
- Possible values:
  - Client: In the operating mode as XAUTH client, the device starts the first phase of the IKE negotiation (main mode or aggressive mode) and then waits for the authentication request from the XAUTH server. The XAUTH client responds to this request with the username and the passphrase from the entry of the PPP table in which the PPP remote terminal corresponds to the VPN remote terminal defined here. It is therefore necessary that there is a PPP remote terminal with the same name as the VPN remote terminal. The username defined in the PPP table typically deviates from the remote terminal name.
  - Server: In the operating mode as a server, the device starts the authentication, after the negotiation of the first IKE has been successful, with a request to the XAUTH client, which then responds with its username and passphrase. The server searches for the transmitted username in the remote terminal names of the PPP table and, if there is a match, checks the passphrase. The username for this entry in the PPP table is not used here.
  - Off: The devices not perform an XAUTH authentication for the connection to this remote terminal.
- Default:
  Off

Note: Set the IKE-CFG option to the same value if you activate the XAUTH authentication for a VPN remote terminal.

6.9 How does VPN operate?

In practice, it is necessary for the VPN to meet a number of demands:
- ☐ Unauthorized third parties are forbidden from reading the data (encryption)
- ☐ Exclusion of data manipulation (data integrity)
- ☐ Indubitable determination of the sender of data (authenticity)
- ☐ Easy handling of keys
- ☐ Compatibility with VPN devices from different manufacturers

VPN achieves these five important goals by using the widely disseminated IPSec standard.

6.9.1 IPSec – the basis for VPN

The original IP protocol does not contain any kind of security precautions. A further complication is that the sender has no possibility for transmitting packets directly to the recipient. Instead, all computers connected to the entire network segment receive these packets. Anyone who wishes to do so can read the packets. That makes abuse of data possible.
Therefore researchers further developed the IP protocol. There is now a secure version: IPsec. VPN is based on IPSec
IPSec stands for "IP Security Protocol" and is originally the name of a working group inside the IETF interest Association, the Internet Engineering Task Force. Over the years, this working group developed a framework for a secure IP protocol, which is now known under the name IPSec.
The important point is that IPSec itself is not a protocol but only the standard for a protocol framework. IPSec consists in fact of a wide variety of protocols and algorithms for encryption, authentication and key management. The following section introduces the standards.

- **Security in IP clothing**
  IPSec is implemented (almost) completely inside layer III of the OSI model, i.e. in the network layer. In IP networks, the traffic of data packets based on the IP protocol takes place in layer 3.
  Thus IPSec replaces the IP protocol. The internal structure of packets under IPSec is different than for IP packets. At the same time, their external structure remains completely compatible with IP. The transport of IPSec packets inside existing IP networks is therefore largely problem-free. The devices in the network responsible for the transport of the packets have no possibility of distinguishing IPSec packets from IP packets by looking at their exterior.
  Certain firewalls and proxy servers that also access the contents of the packets are exceptions. The problems result from (partially functionally-induced) incompatibilities of these devices with the prevailing IP standard. For these devices, an appropriate adaptation to IPSec is necessary.
  The next generation of the IP standard (IPv6) has implemented IPSec. Therefore the assumption has been that IPSec will continue to be the most important standard for virtual private networks in the future as well.

6.9.2 Alternatives to IPSec

IPSec is an open standard. It is independent of individual manufacturers, and the IETF developed IPSec with the inclusion of the interested public. The IETF is open to everyone and does not have any economic interests. The wide recognition of IPSec results from the open design for combining a variety of technical approaches.
There nevertheless were and are different approaches for implementing VPNs. Only the two most important ones will be mentioned here. In contrast to IPSec, which operates on the network layer, they act on the connection and application layer.

- **Security on the connection layer – PPTP, L2F, L2TPthe**
  The possibility of forming tunnels already exists on the connection layer (layer 2 of the OSI model). Microsoft and Ascend developed the Point-to-Point Tunneling Protocol (PPTP) early on. Cisco introduced a similar protocol with Layer 2 Forwarding (L2F). Both manufacturers agreed on a common procedure and the Layer 2 Tunnel Protocol (L2TP) resulted from it in the IETF.
  The advantage of these protocols versus IPSec is primarily that there is a possibility of constructing any desired network protocol on such a secure network connection, in particular NetBEUI and IPX.
  An essential disadvantage of the above described protocols is the lack of security on the packet level. Moreover, these particles were specifically developed for dial-in connections.

- **Security on a higher level – SSL, S/MIME, PGP**
  Communication can be secured by encryption on higher layers of the OSI model as well. Well-known examples for protocols of this type are SSL (Secure Socket Layer), primarily for Web browser connections, S/MIME (Secure Multipurpose Internet Mail Extensions) for e-mail and PGP (Pretty Good Privacy) for e-mail and files.
  In all these protocols an application takes over the encryption of the transmitted data, for example, the web browser on one side and the HTTP server on the other.
  One disadvantage of these protocols is a limitation to certain applications. Additionally, different keys are generally needed for different applications. You therefore manage the configuration on each individual computer. A convenient configuration only at the gateways, as with IPSec, is impossible. To be sure, security protocols on the application layer are more intelligent; after all they know the meaning of the transmitted data. But they are generally also markedly more complex
  All these layer 2 protocols allow only end-to-end connections and are therefore (without extensions) unsuitable for coupling entire networks. On the other hand, these mechanisms do not require any changes to the network devices or the access software. They also have the capability, differently from protocols and other network layers, of being effective even if the data contents have already reached the computer.

- **Combination is possible**
  All the above mentioned alternatives are compatible with IPSec and therefore also applicable in parallel. In this manner there is the possibility of increasing the security level. Thus there is the possibility of dialing into the Internet with an L2TP connection, constructing an IPSec tunnel to a Web server and also exchanging the HTTP data between the Web server and the browser in the secure SSL mode.
  However, each additional encryption impairs the data rate. The user will decide in the individual case whether security over IPSec alone is sufficient. In rare cases, a higher security will in fact be necessary. Particularly since the degree of security to be used can still be adjusted inside IPSec.

6.10 The standards behind IPSec

IPSec Is based on different protocols for different subfunctions. The protocols build on and supplement one another. The modularity achieved by this concept is an important advantage of IPSec over other standards. Since IPSec is not restricted to certain protocols, supplementation with future developments is possible at any time. The protocols so far integrated also offer such a high degree of flexibility that there is a possibility of adapting IPSec perfectly to almost any need.

6.10.1 Modules of IPSec and their tasks

IPSec has a number of tasks to perform. One or more protocols are defined for each of these tasks.

- ☐ Securing the authenticity of the packets
- ☐ Encryption of the packets
- ☐ Transmission and management of the keys

6.10.2 Security Associations – numbered tunnels

A logical connection (tunnel) between two IPSec devices is called an SA (Security Association). The IPSec device manages these SAs independently. An SA consists of 3 values:

- ☐ Security parameter Index (SPI)
  Code number for distinguishing us several logical connections to the same target device with the same protocols.
- ☐ IP target address
- ☐ Security protocol used
  characterizes the security protocol used for the connection: AH or ESP (more on these protocols in the following sections)

Characterizes the security protocol used for the connection: AH or ESP (more on these protocols in the following sections)
An SA applies solely to one communication direction of the connection (simplex). For a full-fledged transmission and reception connection, two SAs are required. An SA also only applies to one protocol in use. If AH and ESP are used, then 2 separate SAs are likewise necessary, i.e., 2 for each communication direction.
The SAs are managed in the IPSec device in an internal database, in which the extended connection parameters are also present. These parameters include, for example, the algorithms and keys that are used.

6.10.3 Encryption of the packets – the ESP protocol

The ESP (Encapsulating Security Payload) protocol encrypts the packets for protection from unauthorized access. The protocol now has additional possibilities for protecting integrity and determining authenticity. ESP also now has effective protection against packet replay. ESP thus offers all the functions of AH.

Mode of operation of ESP

The structure of ESB is more complicated than that of AH. ESP likewise adds a header behind the IP header, but also a trailer of its own and a block with ESP authentication data.

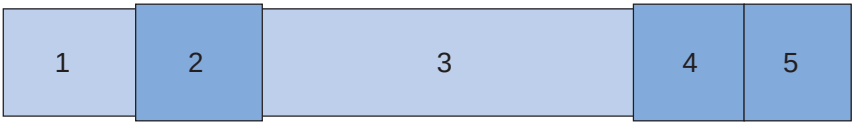


Figure 105:ESP packet

1: IP header
2: ESP header
3: Data
4: ESP trailer
5: ESP auth. data

Transport and tunnel mode

ESP (like AH as well) offers 2 modes Transport mode and tunnel mode. In transport mode, the IP header of the original packet remains identical and the ESP header, the encrypted data and the two trailers are inserted. The IP header contains the constant IP address. Transport mode is therefore suitable only for usage between 2 endpoints, e.g., for remote configuration of a router. If you want to connect networks via the Internet, then transport mode is unsuitable. Here you need a new IP header with the public IP address of the opposite party. In these cases, ESP is used in tunnel mode.

Tunnel mode encrypts the entire packet, including the original IP header, at the tunnel entry, authenticates it and provides it with an ESP header and trailers. This new packet contains a new prefixed IP header, this time with the public IP address of the recipient at the end of the tunnel.

Encryption algorithms

As a higher-level protocol, IPSec does not presume any specific encryption algorithms. The manufacturers of IPSec products are free to choose the methods applied. The following standards are typical:

- AES – Advanced Encryption Standard.
  AES Is the official encryption standard for use in United States government agencies, and therefore the most important encryption technique globally. Following a global competition between numerous encryption logarithms, the National Institute of Standards and Technology (NIST) chose the Rijndael algorithm (pronunciation: "Rine doll") and declared it the AES in 2001.
  The Rijndael algorithm is asymmetrical encryption method that operates with variable block and key lengths. Two Belgian cryptographers, Joan Daemen and Vincent Rijmen, developed this method, which is distinguished by high security, high flexibility and outstanding efficiency.
- DES – Data Encryption Standard
  IBM developed DES in the early 1970s for the NSA (National Security Agency). For many years it was the global encryption standard. The key length of this symmetrical method is 56 bits. Because of its short key length, this method is considered insecure today and thus NIST replaced it in 2000 with AES (Rijndael algorithm). Continuing to use it is discouraged.
- Triple-DES (also called 3-DES)
  Is a refinement of DES. This standard applies the conventional DES algorithm three times in succession. Two different keys with 56 bits each are used, with the key of the first pass being used again in the third pass. This results in a nominal key length of 168 bits and an effective key length of 112 bits.
  Triple DES combines the clever technique of DES with a sufficiently long key and is therefore considered very secure. Triple DES operates more slowly than other methods, however.
- Blowfish
  This development of the prominent cryptographer Bruce Schneier encrypts symmetrically. Blowfish achieves an outstanding data throughput and is considered very secure.
- CAST (named for its authors, Carlisle Adams and Stafford Tavares)
  Is a symmetrical method with a key length of 128 bits CAST allows a variable change of parts of the algorithm during runtime.

Note: You have the possibility of adjusting the encryption under LANconfig. Interventions of this type are usually necessary only if you are setting up VPN connections between devices of different manufacturers. By default, Hirschmann gateways offer encryption either according to AES (128 bits), Blowfish (128 bits) or Triple DES (168 bits).

6.10.4 Authentication – the AH protocol

The AH (Authentication Header) protocol guarantees the integrity and authenticity of the data. We will consider integrity as a separate problem below that the AH protocol solves (not a component of authenticity). In addition to integrity and authenticity, AH also offers effective protection against third-party resending of received packets (replay protection).
AH adds its own header to IP packets directly after the original IP header. The most important component of this AH header is a field with authentication data, also referred to as an integrity check value (ICV).

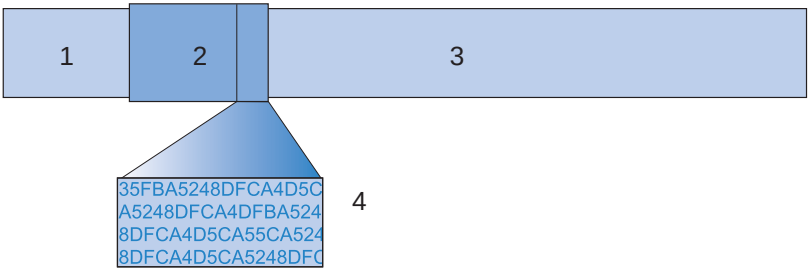


Figure 106:AH header with authentication data
1: IP header
2: AH header
3: Data
4: Authentication data, ICV

The process sequence of AH in the transmitter

The creation of the authentication data in the packet transmitter runs in 3 steps.

- ☐ A checksum is calculated from the total packet by means of hash algorithms.
- ☐ A hash algorithm calculates a new checksum from this checksum, together with a key known to the transmitter and receiver.
- ☐ This results in the sought-for authentication data, which is in the AH header.

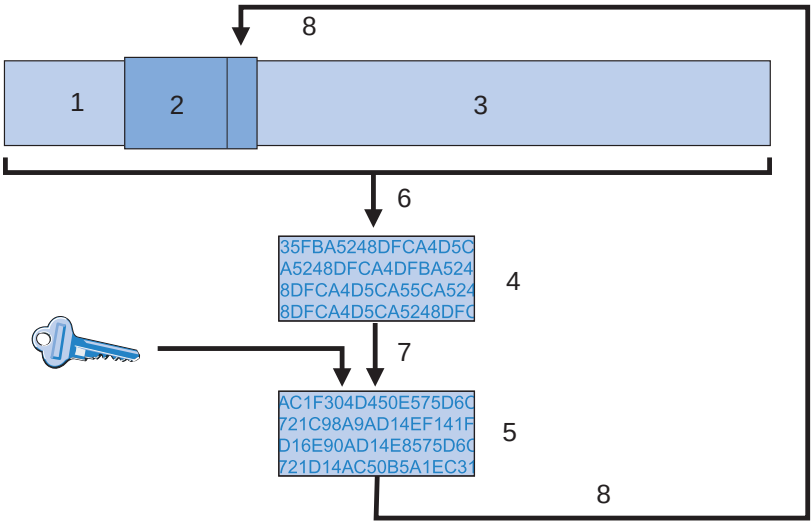


Figure 107:Creation of the authentication data in 3 steps

1: IP header
2: AH header
3: Data
4: Check sum (hash code)
5: Authentication data, ICV
6: Checksum of the entire packet by means of hash algorithm
7: New checksum from old checksum and key
8: Authentication data for AH header

Checking integrity and authenticity in the receiver

The AH protocol runs very similarly in the receiver. The receiver also first calculates the authentication data for the received packet with its key. The comparison to the transmitted ICV of the packet indicates whether the integrity and authenticity of the packet have been preserved.

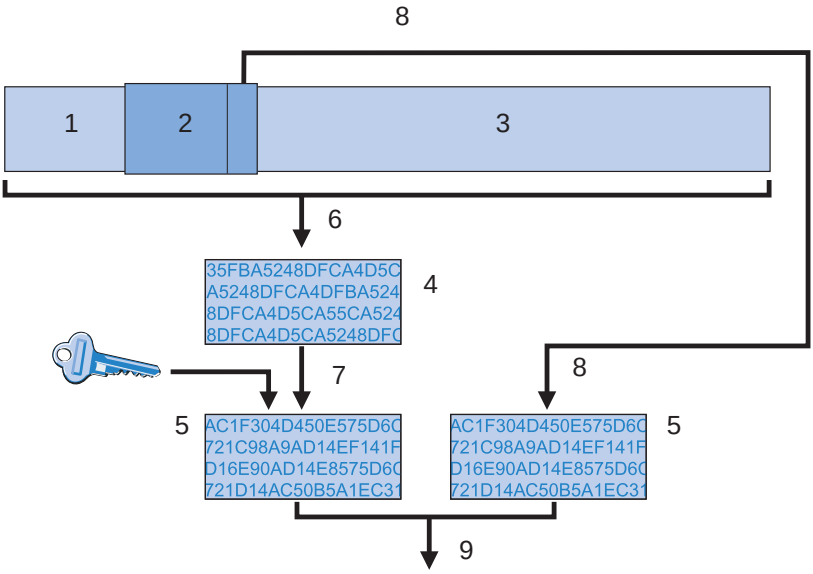


Figure 108:Checking integrity and authenticity in the receiver

1: IP header
2: AH header
3: Data
4: Checksum (hash code)
5: Authentication data, ICV
6: Checksum of the entire packet by means of hash algorithm
7: New checksum from old checksum and key
8: Authentication data of the AH header
9: Check for equality

Forming the checksum for the integrity check

In order to guarantee the integrity, i.e., the correctness of the transferred packets, AH furnishes each packet with a checksum when it is transmitted. In the receiver, AH checks whether the checksum matches the content of the packet. If it does not match, then there was either a transmission error or someone deliberately changed the data. AH immediately rejects such packets so that they do not reach any higher protocol level.

Various so-called hash algorithms are available for calculating the checksum. Hash algorithms are distinguished by the fact that the results (the hash code) are characteristic of the input data ("fingerprint"). Conversely, it is impossible to infer the input data from the hash code. With a high-quality hash algorithm, even the slightest changes of the input value result in a completely different hash code. This makes systematic analyses of several hash codes difficult.

VPN supports the two most common hash algorithms: MD5 and SHA-1. Both methods operate without keys, i.e., solely on the basis of fixed algorithms. Keys come into play only in a later step of AH: in the final calculation of the authentication data. The integrity checksum is only a necessary interim result on the way to the calculation.

Calculation of the authentication data

In this second step, AH forms a new hash code, the final authentication data, from the checksum and a key. For this process as well, there are different standards that can be selected under IPSec. VPN supports HMAC (Hash-based Message Authentication Code). The hash functions MD5 and SHA-1 are available as hash algorithms. The HMAC versions are accordingly called HMAC-MD5-96 and HMAC-SHA-1-96.

It now becomes clear that AH itself leaves the packet unencrypted. Only the checksum of the packet and one's own key are encrypted together into the ICV, the authentication data and added to the packet as the check criterion.

Replay protection – protection from repeated packets

In addition to the labeling with the ICV, AH marks each package with an unambiguous sequence number. Thereby the receiver has the possibility to recognize those packets that a third party has received and is now sending again. This type of attack is called "packet replay."

Note: Masking of IPSec tunnels is not possible with AH unless additional measures such as NAT traversal or an external layer 2 tunneling (e.g., PPPT/LPT2) again provide a "changeable" external IP header.

6.10.5 Management of the keys – IKE

The Internet Key Exchange Protocol (IKE) is a protocol with which there is the possibility of incorporating subprotocols for constructing SAs and for key management.
VPN uses 2 subprotocols inside of IKE: Oakley for the authentication of the partners and the key exchange, as well as ISAKMP for managing the SAs.

- **Construction of the SA with ISAKMP/Oakley**
  Every construction of an SA takes place in several steps. For dynamic Internet connections, these steps take place after the transmission of the public IP address. The steps are:
  - ☐ The initiator sends a message via ISAKMP to the remote terminal in clear text with the request to set up an SA and proposals for the security parameters of this SA.
  - ☐ The remote terminal accepts this proposal.
  - ☐ Both devices now generate number pairs (consisting of a public and a private numerical value) for the Diffie-Hellman method.
  - ☐ The two devices exchange their public numerical values for Diffie-Hellman in 2 additional messages.
  - ☐ From transmitted numerical material (according to the Diffie-Hellman method) and the shared secret, the two sides generate a common secret key with which they encrypt further communication. The two sides additional mutually authenticate themselves using hash codes of their shared secret. The so-called phase 1 of the SA construction is thus ended.
  - ☐ Phase 2 is based on the encrypted and authenticated connection that was set up by the devices in phase 1. In phase 2 they generate and transmit the session keys for the authentication and symmetric encryption of the actual data transfer.

Note: Use symmetric methods for encrypting the actual data transfer. Asymmetric methods (also known as public-key encryption) are more secure, since the devices do not transmit any secret keys, but require expensive calculations and are therefore markedly slower than symmetric methods. In practice, public-key encryption is usually used on only for exchanging key material. The actual data encryption then takes place with fast symmetric methods.

- The regular exchange of new keys
  ISAKMP ensures during the existence of the SA that the devices exchange new key material with one another on a regular basis. This process takes place automatically. You have the possibility of controlling this process via the setting for "lifetime" in the extended configuration of LANconfig.

6.11 Improved phase 1 rekeying

During a VPN connection, the participating stations continually check whether the communication is always performed according to a previously agreed security association (SA). If the framework conditions change (e.g. change of IP address of client due to change of location to different radio cell), you set up this security association again by what is known as “rekeying”.
From version 2.30 on, the Lancom Advanced VPN Client transmits a special identification number (ID) during the phase 1 rekeying. Using this ID, a Hirschmann VPN gateway detects the rekeying and connects the previously negotiated security association with the logged in client. Therefore, the re-authentication, usually compulsory, is not required.

6.12 Intelligent Precalculation of DH Keys

The negotiation of a VPN connection is based on the creation of keys according to the Diffie-Hellman method. Depending on the key length, however, calculating a DH key can take some time. If a VPN gateway temporarily loses its Internet connection, the recalculation of all the DH keys may incur a delay before all of the VPN clients can reconnect to the VPN gateway.

With the precalculation of DH keys, the device can accelerate the renegotiation of VPN connections. The precalculation and the number of keys to be generated are set up in WEBconfig:

`HiLCOS Menu Tree:Setup:VPN:Isakmp:Groups`

The precalculation of keys has a low priority. When the CPU of the device is not busy with other, higher priority tasks, it builds up a stock of public DH keys.

6.13 MPPE encryption for PPTP tunnel

The MPPE encryption protocol (Microsoft Point-To-Point Encryption) secures the data transmission via PPP and VPN connections with key lengths of up to 128 bits.
For the encryption, MPPE uses what is known as the “Stateless Mode” to ensure the synchronization of the two communication partners. In this mode, the session key changes with every transmitted data packet. Additionally, each time the two stations synchronize their encryption tables, in which the keys for the data encryption are stored.
VPN-capable Hirschmann devices use MPPE as a means of encrypting the data transmission via PPTP tunnels.
In LANconfig, you will find this setting under `Communication:Protocols:PPTP List`.
If you have activated the MPPE encryption protocol, the device only sets up connections with clients under the following conditions:

- The client wants to set up an MPPE-secured connection. With other protocols, the router rejects a connection.
- The client uses a minimum of the key length specified in the router. If the key length is smaller, the router rejects a connection, and if the encryption is stronger, the router switches to the corresponding key length.

6.13.1 Enhancements in the menu system

Encryption
Here you enter the key length.

- **SNMP ID:**
  2.2.21.7
- **Telnet path:**
  `Setup:WAN:PPTP Remote Devices`

- **Possible values:**
  Off
  40 bit
  56 bit
  128 bit
- **Default:**
  Off

7 Security

Security is an important topic in the configuration of an OpenBAT device.

7.1 A WLAN Security Overview

7.1.1 Basic Considerations

The following elements should be considered when developing a security plan for your wireless network:

- **Authentication**

  Authentication is used to grant network access to authorized network users.

  Authentication can be implemented, for example, using certificates or passwords.

- **Authenticity**

  Authenticity encompasses the proof of authorship and originality of data content. Authentication is the process of establishing this proof.

- **Integrity**

  After access has been granted, data packets need to reach the target without any falsification.

- **Confidentiality**

  Confidentiality involves shielding data traffic from unauthorized third parties. This is achieved by encrypting the data.

7.1.2 IEEE 802.11i /WPA2

The IEEE standard 802.11i—WiFi Protected Access 2 (WPA2)— provides a heightened standard of security for WLANs. WPA2 enables IEEE 802.1X authentication and authorization of users. It also supports AES encryption, which is a far more secure technique than WEP or WPA.

7.1.3 TKIP and WPA

The original WPA standard specifies TKIP/Michael as an encryption method. With the further development of the 802.11i standard, the AES/CCM method was added. In a WPA network it is possible for some clients to communicate with the access point using TKIP, while other clients use AES.

7.1.4 WEP

WEP offers far lower security than IEEE 802.1x/WPA2. OpenBAT devices continue to support this encryption method in order to be compatible with older client devices that exclusively support the WEP protocol. However, Hirschmann expressly recommends use of a better method for securing the WLAN (e.g., IEEE 802.1X/ WPA2).

7.1.5 LEPS: LANCOM Enhanced Passphrase Security

LEPS increases global passphrase security

WPA and IEEE 802.11i encryption provide WLAN data traffic with greater security against eavesdropping than the older WEP method.

LEPS provides an efficient method that makes use of the simple configuration of IEEE 802.11i. LEPS uses an additional column in the access control list (ACL) to assign an individual passphrase to each MAC address. The connection to the access point and the subsequent encryption with IEEE 802.11i or WPA is achieved by using the correct combination of passphrase and MAC address.

Configuring LEPS

To configure a WLAN client for LEPS, do the following:

- ☐ Enable MAC filtering for the access point:
  - ☐ In the `Configuration : Wireless LAN : General` dialog click 'Logical WLAN settings...' and select a wireless network.
  - ☐ In the `Logical WLAN settings : Network` dialog, select 'MAC filter enabled'.
- ☐ Add a unique passphrase to each client station:
  - ☐ In the `Configuration : Wireless LAN : Stations` dialog, click 'Stations...'.
  - ☐ In the `Stations` window, select a station and click 'Edit...'
  - ☐ In the `Stations : Edit Entry` dialog, enter a unique 'Passphrase' for the client station.

7.1.6 Background WLAN Scanning

A OpenBAT device in the role of access point actively scans the available wireless channels (just as a WLAN client does when searching for an available access point). If the OpenBAT device detects another active access point, that device's relevant information is recorded in the scan table. Because this scan/record process occurs in the background during the normal radio activity of the access point, it is called a background scan.

Background scanning is primarily used to detect:

- rogue access points
- fast roaming clients

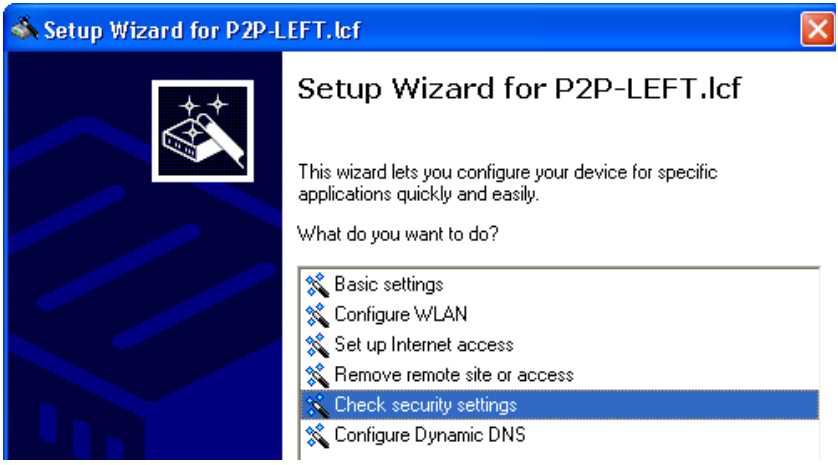
Evaluating the Background Scan

Use LANmonitor to view the results of background scanning. You can use the tools within LANmonitor to group detected access points, and provide e-mail notification whenever a new WLAN access point or client is detected.

7.2 Securing the Configuration

Many parameters for the security of your network and the authorizations for individual network users are established in the configuration of the device. These parameter settings should not be changed by unauthorized persons. These security-related settings can be configured individually, or by means of the 'Check security settings' wizard.

7.2.1 Using the Check Security Settings Wizard


Setup Wizard for P2P-LEFT.lcf
Setup Wizard for P2P-LEFT.lcf
This wizard lets you configure your device for specific applications quickly and easily.
What do you want to do?
Basic settings
Configure WLAN
Set up Internet access
Remove remote site or access
Check security settings
Configure Dynamic DNS

Use the ’Check Security Settings’ wizard to step through the process of securing your OpenBAT device configuration, including:

- Passwords (see on page 511)
- Login barring (see on page 513)
- Selection and configuration of an encryption method:
  – WPA, or
  – WEP
- SSID assignment
- Controlling access to the configuration settings from (see on page 514):
  – remote networks
  – the wireless network (WLAN)
  – the local area network (LAN)
- Controlling access to the configuration settings by IP address (see on page 516)
- Activating the following firewall features:
  – stateful inspection firewall
  – ping blocking
  – stealth mode

Many of these settings can also be set by the ’Basic settings’ and ’Configure WLAN’ wizards. These settings can be independently configured in the LANconfig or the WEBconfig software.

7.2.2 Passwords

The simplest way to help secure the configuration is to assign a password.

Note: If a password has not been set:

- Anyone can access and change the configuration of the device.
- The LED flashes at regular intervals until the device has been configured correctly.

Note: The combination of user and password can also be used for both Telnet and HyperTerminal access.

Configuring the Password

The 'Main device password' can be set in the 'Device configuration' section of the `Configuration : Management : Admin` dialog. The default password setting is 'private'.

Requiring a Password for SNMP Read Access

When you set the password, you should also select the 'Password required for SNMP read permission' setting in the same dialog.

7.2.3 Login Barring

The OpenBAT device can be configured to frustrate brute force attacks. A brute-force attack is the attempt by an unauthorized person or device to decipher a password and gain access to a network. A brute force attack involves multiple login attempts, using all possible combinations of letters and numbers until the right password is found. To guard against brute force attacks, configure the following settings in the "Configuration Login Lock" section of the `Configuration :, Management : Admin`:

☐ Lock configuration after: Type in the number of login attempts that will lock the device configuration.

☐ Lock configuration for: Type in the duration of the device configuration lockdown, in minutes.

Note: If barring is activated on any one port, all other ports are also barred.

7.2.4 Restricting Configuration Access Rights

Access to the internal functions of the devices can be restricted separately for each access source, as follows:

- local area network (LAN)
- wireless LAN (WLAN)
- remote networks

For network-based configuration access, further restrictions can be made—for example, specified IP addresses or dedicated LANcapi clients are exclusively allowed access.

The following internal functions are separately selectable:

- LANconfig
- WEBconfig

- SNMP
- Terminal/Telnet

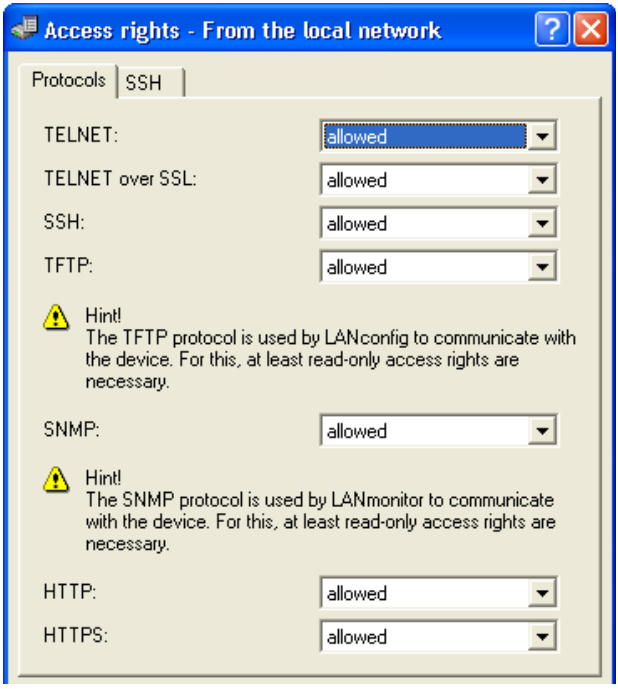
Limiting Configuration Access by Access Source

Access to internal device functions can be controlled based on the access source—LAN, WLAN or remote networks—for individual configuration services. Configuration access can be allowed, denied, or read-only.
To configure these access rights:

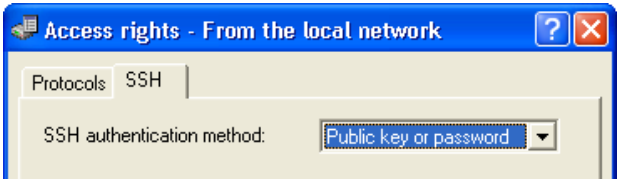
☐ Open the `Configuration : Management : Admin` dialog.

☐ In the 'Configuration access ways' section, click 'Access rights' and then also select an access source:
  – from the local network
  – from the wireless LAN
  – from remote networks

☐ In the 'Access rights' dialog, click on the Protocols tab to display that dialog (below):



- ☐ Use this dialog to grant or deny access rights from the selected access source.
- ☐ Click on the SSH tab to display a dialog where you can select an authentication method for secure shell (SSH) transmissions:



Limiting Configuration Access by IP Address

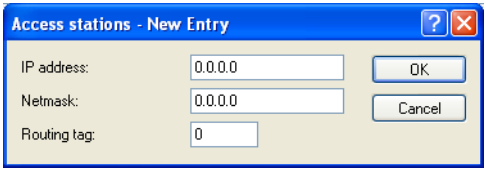
Access to the configuration can also be controlled by creating an IP address filter list. Stations with an IP address included in this list exclusively can access the configuration. To create a station filtering list:

☐ Navigate to the following dialog:`Configuration : Management`. Click the 'Access stations' button.

☐ In the ’Access stations’ window, click ’Add...’.

☐ In the ’Access stations - New Entry’ dialog, enter the following information for each station:
- IP address
- Netmask
- Routing tag

Note: If you specify a routing tag for this access station, it will accept exclusively those packets that were marked with the same tag in the firewall or which arrived via a network with a suitable interface tag. If the routing tag is 0, any access with a suitable IP address is allowed. The use of routing tags is advisable when combined with the corresponding accessory rules in the firewall or tagged network interfaces.



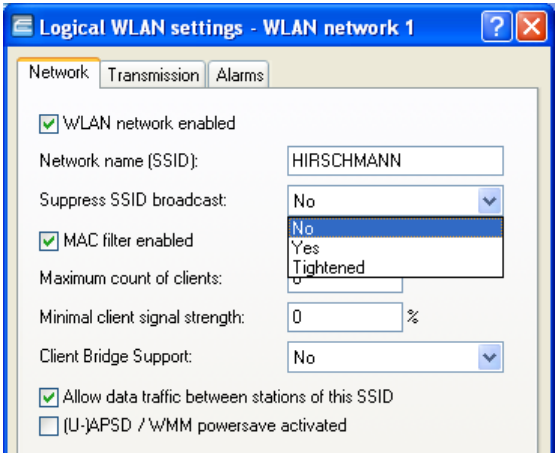
By default, this table does not contain entries. Thus the device can be accessed over TCP/IP from computers with any IP addresses. With the first entry of an IP address (as well as the associated net mask) the filter is activated, and solely the IP addresses contained in this entry are entitled to use the internal functions then. With further entries, the number of the entitled ones can be extended. The filter entries can designate both individual computers and whole networks.

7.2.5 Closed-network Function: Suppress SSID broadcast

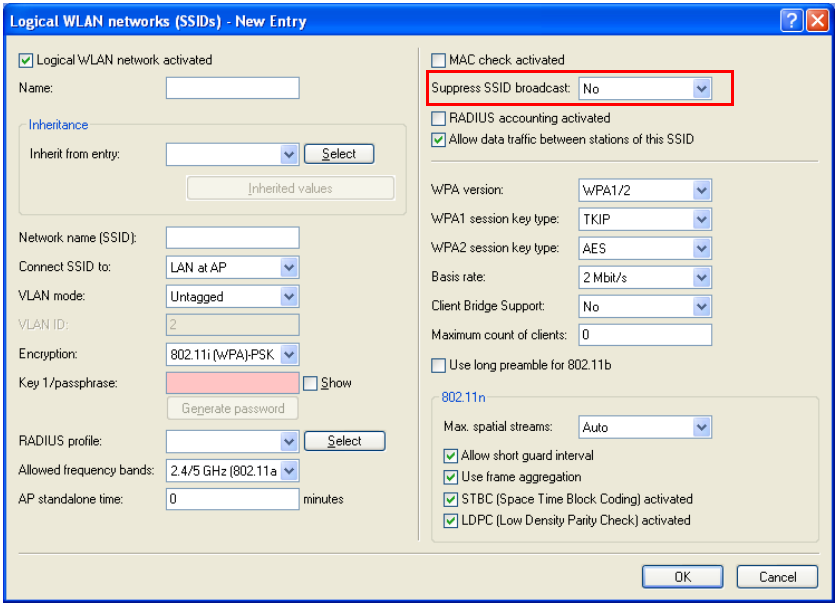
A WLAN client can only connect to a wireless network if it is informed of the corresponding SSID. The state on delivery for many wireless networks allow the use of a blank SSID or the SSID "any", and continuing to use this means that potential intruders do not need to know the SSID of the wireless LAN. The closed network function prevents unauthorized WLAN clients from logging into the WLAN. The access point rejects any attempt to log on with a blank SSID or the SSID "any". Any user wanting to logon to the WLAN must know the correct SSID.

Note: Simply suppressing the SSID broadcast does not provide adequate protection: When legitimate WLAN clients associate with the access point, this transmits the SSID in plain text so that it is briefly visible to all clients in the WLAN network.

LANconfig: `Wireless LAN:General:Interfaces:Logical WLAN settings:Network`.



LANconfig: `WLAN Controller:Profiles:Logical WLAN networks (SSIDs)`



The option "Suppress SSID broadcast" provides the following settings:

- **No**: The access point publishes the SSID of the cell. When a client sends a probe request with a blank or incorrect SSID, the device responds with the SSID of the radio cell (publicly visible WLAN).
- **Yes**: The access point does not publish the SSID of the cell. When a client sends a probe request with an empty SSID, the device similarly responds with an empty SSID. The client cannot log on to the radio cell.
- **Tightened:** The access point does not publish the SSID of the cell. When a client sends a probe request with a blank or incorrect SSID, the device does not respond. The client cannot log on to the radio cell. This setting also reduces the network load if there is a large number of WLAN clients in the radio cell.

8 Virtual LANs

8.1 What is a Virtual LAN?

The increasing availability of inexpensive layer 2 switches makes it possible to design LANs that are much larger than in the past. Until now, smaller parts of a network were connected using hubs. These individual segments—collision domains—had been connected via routers to the wider network. Because a router constitutes the border between two LANs, several LANs with their own IP address ranges arose using this design.

By using switches, you can combine many more stations to one large LAN. By confining the flow data to individual switch ports, the available bandwidth can be utilized more efficiently than with hubs; the need to configure and maintain routers within the network is avoided.

However, a network structure based on switches also presents certain disadvantages:

- Broadcasts are sent over the entire LAN, even if the broadcast data packets relate to just a small segment of the LAN. The increased number of network stations transmitting broadcasts leads to a reduction of available LAN bandwidth.
- All data traffic on the physical LAN is public. Even if individual segments are using different IP address ranges, each station on the LAN is theoretically able to tap into data traffic from all logical networks on the Ethernet segment. The need to secure individual LAN segments using firewalls or routers increases the amount of network administration.

One approach to this situation is the use of virtual LANs (VLANs), as described in IEEE 802.1p/q. Several VLANs can be configured for a single physical LAN. No VLAN obstructs another VLAN, and no VLAN receives or taps into the data traffic of another VLAN on the physical Ethernet segment.

8.2 Configuring VLANs

Adding a OpenBAT device to a VLAN involves the following configuration tasks:

- Defining the VLAN by assigning it a name, giving it a VLAN ID, and identifying the interfaces over which the VLAN operates.
- Defining for each VLAN interface how to handle data packets with and without VLAN tags.

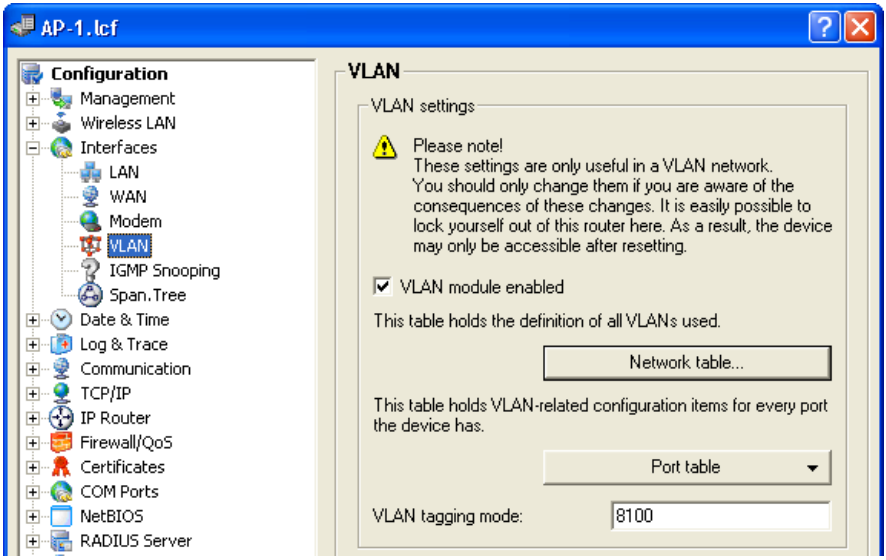
8.2.1 VLAN and ARF

In some cases it is sufficient to configure VLAN settings on the basis of the IP network, using a technique called advanced routing and forwarding (ARF). Using ARF, a VLAN ID is defined for an IP network. All outbound packets from this network are tagged with this VLAN ID. Incoming packets need to be tagged with this VLAN ID in order to be assigned to the network. Details are contained in section on ARF "Advanced Routing and Forwarding." Please observe the information there (see on page 560).

8.2.2 General VLAN Settings

To enter general VLAN settings, follow these steps:

☐ Navigate to the following dialog:`Configuration : Interfaces`. Open the `VLAN` dialog:



☐ Configure the following VLAN settings:

Note: These settings should be edited only by persons with expert level understanding of VLAN operation. Mistaken editing of these VLAN settings can result in the inability to access the OpenBAT device. In such a case, you need to reset the device to regain access.

- VLAN module enabled:
  Select this to activate VLAN support for the OpenBAT device.
- VLAN tagging mode:
  Enter a 16 bit hexadecimal value for the VLAN tag (Ethernet II type). The default value is 8100 (representing 802.1p/q VLAN tagging). Other values for VLAN tagging include 9100 and 9901.

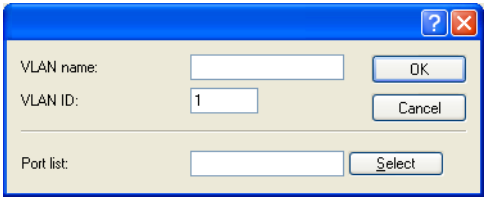
Note: When operating VLAN tagged networks over provider networks that use additional VLANs themselves, providers often use special VLAN tagging IDs, which are entered here as the ‘VLAN tagging mode’.

8.2.3 The Network Table

Use the Network table to define VLANs for the OpenBAT device as follows

☐ Open the `Configuration : Interfaces : VLAN` dialog and click ‘Network table...’

☐ In the ‘Network table’, click ‘Add...” to open the ‘New Entry’ dialog:



☐ Configure the following settings for each VLAN:

- VLAN name:
  The VLAN name serves as a description during configuration. This name is not used in any other place.
- VLAN ID:
  An integer, from 1 to 4094, that serves as a unique identifier for the VLAN.
- Port list:
  Enter every OpenBAT device interface that belongs to this VLAN.

  For a device with a LAN interface and a WLAN port, this setting might contain the entry ‘LAN-1, WLAN-1’.

  To add a port range, enter the beginning and ending port separated by a tilde: ‘P2P-1~P2P-4’.

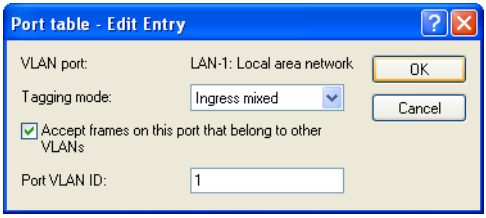
Note: The first SSID of the first WLAN module is named WLAN-1, the other SSIDs are WLAN-1-2 up to WLAN-1-8. If the device has two WLAN modules the SSIDs are WLAN-2, WLAN-2-2 up to WLAN-2-8.

8.2.4 The Port Table

Use the port table to configure each port that is used by the VLAN, as follows:

☐ Navigate to the following dialog:`Configuration : Interfaces: VLAN` dialog:

☐ Click ‘Port table’, then select a port from the list to open the following dialog for that port:



☐ Configure the following settings for each VLAN port:

- Tagging mode:
  Specify how VLAN tags will be assigned and processed over this port. Selections include:

  Never: Outbound packets are not given a VLAN tag at this port. Incoming packets are treated as though they have no VLAN tag. If incoming packets have a VLAN tag, it is ignored and treated as though it were part of the packet's payload. Incoming packets are assigned to the VLAN defined for this port.

  Ingress mixed: Incoming packets may or may not have a tag, but outgoing packets do not obtain a tag. This mode is mainly required for configuration conversion (see below).

  Mixed: Allows mixed operation of packets with and without VLAN tags at the port. Packets without a VLAN tag are assigned to the VLAN defined for this port. Outgoing packets are given a VLAN tag unless they belong to the VLAN defined for this port.

  Always: Outgoing packets obtain a tag, regardless of whether they belong to the port VLAN or not. Incoming packets need to contain a tag—untagged packets are discarded.

- Accept frames on this port that belong to other VLANs:
  This option defines whether tagged data packets with any VLAN ID should be accepted, even if the port is not a ‘member’ of the VLAN.

- Port VLAN ID:
  This setting has two functions:

  Untagged packets received at this port in 'Mixed' or 'Ingress-mixed' mode are assigned to this VLAN, as are all ingress packets received in 'Never' mode.

In the 'Mixed' mode, this value determines whether outgoing packets receive a VLAN tag or not: Packets assigned to the VLAN defined for this port are not given a VLAN tag; all others are given a VLAN tag.

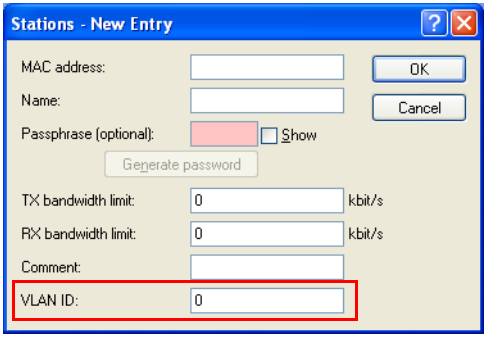
8.3 Configuring VLAN IDs

8.3.1 Assigning Different VLAN IDs to WLAN Clients

VLANs are usually connected to a LAN interface on the OpenBAT device. Therefore, all packets that pass through this interface receive the same VLAN ID when the VLAN module is enabled. However, in some cases, you may want to assign individual WLAN stations to different VLANs. To assign an individual WLAN client station to a specific VLAN:

☐ Navigate to the following dialog:`Configuration : Wireless LAN`. Open the `Stations` dialog and click ‘Stations’.

☐ In the ‘Stations’ dialog, select a station and click ‘Edit’:

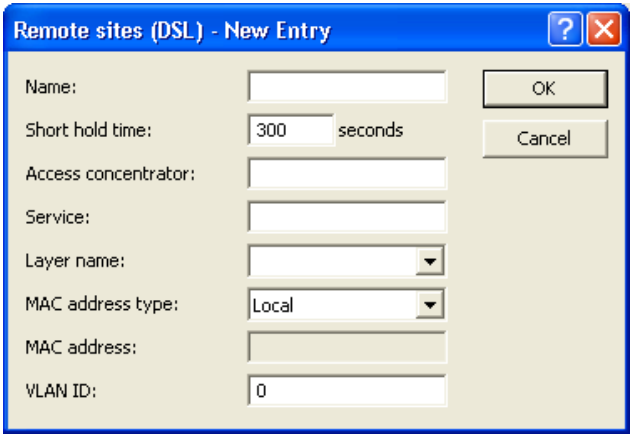


☐ In the ’VLAN ID’ field, enter the identifier that applies to this station.

8.3.2 Special VLAN ID for DSL Interfaces

In order to better separate the data traffic on a DLS interface from other traffic, 'VLAN ID' can be set up independently for a DSL interface in the LANconfig software as follows:

- ☐ Open `Configuration : Communication : Remote Sites` and click ‘Remote sites (DSL)...’
- ☐ In the ‘Remote sites (DSL)’ window, click ‘Add...
- ☐ In the ‘Remote sites (DSL) - New Entry’ dialog, in the ‘VLAN ID’ field, enter the specific ID of the VLAN so that it can be uniquely identified over the DSL connection.



8.4 VLAN Tagging on Ethernet Layers 2 and 3

8.4.1 Introduction

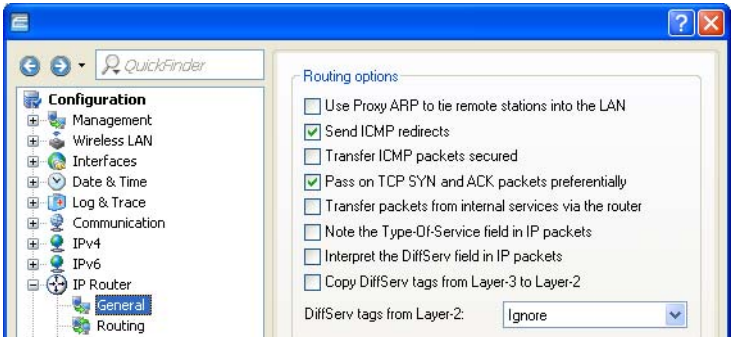
VLANs operate on the Data Link Layer (layer 2) of the OSI model. However, you can configure the OpenBAT device to transfer VLAN tags to the DSCP fields (Differentiated Services Code Point - DiffServ) and/or the priority setting in the TOS field (Type of Service), both of which operate on the Network Layer (layer 3). The processing of VLAN tagged packets requires that packets in the receive direction are regarded differently from packets in the send direction.

Note: When a tagged packet is received, the tag is saved to the associated entry in the connection list. If a packet is to be sent with a priority setting, the VLAN ID recorded earlier is entered into the packet together with the priority to form a VLAN tag. Where a connection causes other connections to be opened—e.g. with ftp or H.323—the tag is inherited by the new entries.

8.4.2 Configuration of VLAN tagging on layer 2/3

Configuration of the transfer of VLAN tags between layer 2 and layer 3 elements of the IP data packet is accomplished by entering routing settings as follows:

☐ Navigate to the following dialog:`Configuration : IP-Router:` Open the `General` dialog.



☐ Specify how TOS/DiffServ tags will be routed:

– Select "Note the Type-Of-Service field in IP packets" to enable ToS checking. The OpenBAT device checks the bits for particularly fast or secured transmission.

– Select "Interpret the DiffServ field in IP packets" to enable DiffServ checking. The OpenBAT device checks the bits for Class Selector, Assured Forwarding, and Expedited Forwarding settings.

– De-select both of these settings (the default setting), and the device will not transfer VLAN tags between layers 2 and 3.

Note: De-selecting both of these fields will also disable QoS for the device.

☐ Use the ‘Copy DiffServ tags from Layer-3 to Layer-2’ settings to regulate device behavior when it transmits a data packet. If this option is selected, VLAN tags with priority bits originating from the DSCP precedence will be generated if the recipient has previously sent at least one tagged packet.

☐ Use the ‘DiffServ tags from Layer-2’ setting to regulate device behavior when it receives a data packet:

- Ignore: Turns off layer-2 to layer-3 VLAN tag transfer.
- Copy to Layer-3: Priority bits in the VLAN tag are copied to the precedence of the DSCP.
- Copy automatically: Priority bits in the VLAN tag are copied exclusively to the DSCP precedence if this is '000'.

9 LLDP

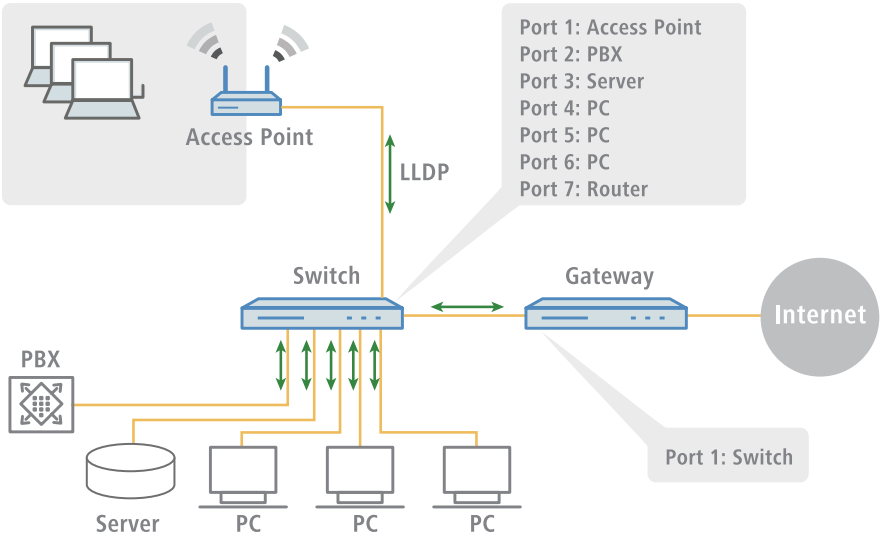
The Link Layer Discovery Protocol (LLDP) provides a simple and reliable way to exchange information between neighboring devices on the network and for determining the topology of networks. LLDP provides discovery functions to identify individual devices and entire network structures using the procedures defined in the IEEE 802.1AB standard. Since the protocol works on Layer 2 (security level) of the OSI layer model and it is, therefore, used for physically addressing devices, its functionality is not limited to logical networks such as IP networks. In principle, LLDP covers all physically accessible devices on the network.

In particular, the vendor-independent LLDP protocol offers many advantages in complex networks:

- It enables the automatic detection of components attached to a network such as routers, switches, and WLAN access points.
- It simplifies the integration of a wide range of different devices, which support the LLDP standard, into an existing network: Using central network management software, and automatic testing and diagnostic processes, the time required for setup, operation and maintenance of a network is reduced.
- The information sent by the individual devices provides an overview of the topology (i.e., structure and arrangement) of the entire network. Central management software provides the administrator with a virtual image of the network, which is automatically updated when there are changes in the topology.
- With the help of management software, the administrator can also easily monitor and manage complex networks. Using this software, he can determine which components and devices are interconnected and can easily locate any faults.
- LLDP can reduce the costs of buying, building or restructuring a network, since companies are no longer dependent on specific manufacturers because of this open standard. Individual network components can be selected based on which one is best for your implementation. This was previously not possible when proprietary protocols were in use.

9.1 How it works

LLDP works on a simple principle: The so-called LLDP agent runs on all devices with LLDP support. On the one hand, this software component sends information to all interfaces of the device at regular intervals. This is done using either Unicast or Multicast, depending on the destination addresses, which you can configure as required. On the other hand, the LLDP agent is continuously receiving information from neighboring devices. The transmission and reception of the respective data packets is handled independently from each other.



The data packets being sent and received contain information such as the name and the description of the device, the ID and description of ports, the IP address or MAC address of the device, the specific capabilities of the device (e.g., in terms of switching and routing), VLAN identifiers and vendor-specific details. In this case, LLDP defines basic information that a data packet must always include, as well as optional additional information.

The individual devices store the information received locally in a data structure, the so-called MIB (Management Information Base). An MIB therefore contains data from its own LLDP agent and of the detected, direct neighbor agent.

The information exchange provides a continuing identification of the devices within the network, because the devices normally send packets cyclically (i.e. in configurable intervals). Furthermore, the devices also inform their network neighbors when changes occur on the device or in its network connection.

For the actual device identification process it is crucial that each connection point in the topology is clearly identified as a "Media Service Access Point" (MSAP). An MSAP is composed of a device ID (Chassis ID) and a port identification (Port ID). The unique identification or assignment of devices is therefore based on the fact that each MSAP in the monitored network topology may occur only once.

The Administrator can query and capture the data reported by the devices via a central network management software on his computer, where the query of the individual MIBs is performed using the SNMP protocol. The management software thus documents the entire topology of the network and allows automatic display of this topology along with a graphic representation of the current diagnostic data.

9.2 Structure of LLDP Messages

Information is exchanged using specific units of data known as LLDP Data Units (LLDPDU). These data unit consists of TLVs (Type-Length-Values), and each TLV field corresponds to a certain type and has a certain length.

In accordance with the LLDP standard IEEE 802.1AB three TLVs are mandatory at the beginning of an LLDPU in the following order:

- Type 1 = Chassis ID
- Type 2 = Chassis ID
- Type 3 = Time to live

Following these mandatory TLVs, an LLDPDU can include additional, optional TLVs:

- Type 4 = Port description
- Type 5 = System name
- Type 6 = System description

- Type 7 = System capabilities
- Type 8 = Management address

At the end of an LLDPDU the following TLV is mandatory:

- Type 0 = End of LLDPDU

Tab. 2: Tabular overview of the TLVs

TLV	Usage	Name	Example	Function
Type 1	Required	Chassis ID	0018.2fa6.b28c	Identifies the device
Type 2	Required	Port ID	Fi-0/12	Identifies the port
Type 3	Required	Time to live	60 sec	Signals to the receiving device how long the received information should remain valid
Type 4	Optional	Port description	GigabitEthernet0/12	Displays details about the port such as the hardware version
Type 5	Optional	System Name	PN-I/O 3	Displays the name given to the device by the administrator
Type 6	Optional	System description	HiLCOS software, version 8.9.1 SE	Displays details about the device such as the version of the networking software
Type 7	Optional	System capabilities	Router	Displays the primary function and capabilities of the device.
Type 8	Optional	Management address	192.168.0.1	Shows the IP or MAC address of the device
Type 0	Required	End of LLDPDU	----------	Signals the end of the data unit

9.3 Supported Operating Systems

In principle, LLDP works on all popular systems, provided that LLDP agents or an appropriate software for evaluation of the LLDP packets is available. For Linux there are various open source projects, such as "LLDPD", "Open-LLDP" (with hyphen) or "ladvd", which deploy an LLDP agent.

The project "OpenLLDP" aims to achieve a further dissemination and acceptance of the LLDP protocol (802.1AB). The software supports the transmission and reception of LLDP messages on the Linux, Mac OS X, FreeBSD, and NetBSD platforms. Currently, however, this development seems to be stalled.

Microsoft Windows Vista and Windows 7 contain a proprietary protocol called LLTD (Link Layer Topology Discovery), which is essentially the same functionality as LLDP. On Windows XP, the LLTD component can be installed later as a patch. However, the patch is limited compared to the features implemented in Vista and Windows 7 because the "LLTD Responder" only reports IPv4 addresses, and not IPv6 addresses.

If you want to install LLDP on Windows systems, you can use a shareware called "haneWIN LLDP Agent". Using this, LLDP works on all Windows systems as of Windows 2000, i.e., on both 32-bit and 64-bit systems.

The most widely used free software for evaluation and analysis is Wireshark. The basic version of Wireshark is free of charge and now well-established as a standard. The software supports a wide variety of operating systems and can read and evaluate a wide variety of protocols (including LLDP). However, the focus of the basic version of Wireshark is the analysis of problems within the network. If you need more features (such as the visualization of network traffic in the form of colored graphs), you can purchase add-on modules.

9.4 Configuration

LLDP configuration via WEBconfig. For further information, see the CLI reference material.

`HiLCOS menu tree : Setup : LLDP`

10 Routing and WAN Connections

This chapter describes WAN protocols, and shows you how to configure and optimize WAN connections.

10.1 General aspects of WAN connections

WAN connections are used for the following applications:

- Internet access
- LAN to LAN coupling
- Remote access

10.1.1 Bridges for Standard Protocols

WAN connections differ from direct connections in that the data in the WAN are transmitted via standardized network protocols also used in the LAN. Direct connections, on the other hand, operate with proprietary processes that have been specially developed for point-to-point connections.

WAN connections extend a LAN. WAN connections form a kind of bridge for the communication between networks (or for connecting individual computers to the LAN). By contrast, a direct connection establishes just a single connection from one individual PC to another PC.

WAN Connection Protocols

WAN connections over high speed ports (e.g. DSL connections) use the IP standard for transmitting packets.

WAN Connections and the Router

WAN connections characteristically interact with the router modules in the OpenBAT device. The router modules (IP and IPX) provide the connection to LAN and WAN. They use the WAN connections to respond to requests for external resources, made by PCs within the LAN.

10.2 IP Routing

An IP router operates between networks that use TCP/IP as the network protocol. This allows data transmissions exclusively to destination addresses that are entered in the routing table. This section explains the structure of the IP routing table in a router, as well as the additional functions available to support IP routing.

10.2.1 The Routing Table

The IP routing table informs the router to which remote station (other router or computer) the router should send the data for a particular IP address or an IP address range. This type of entry is known as a ‘route’ because it is used to describe the path of the data packet.

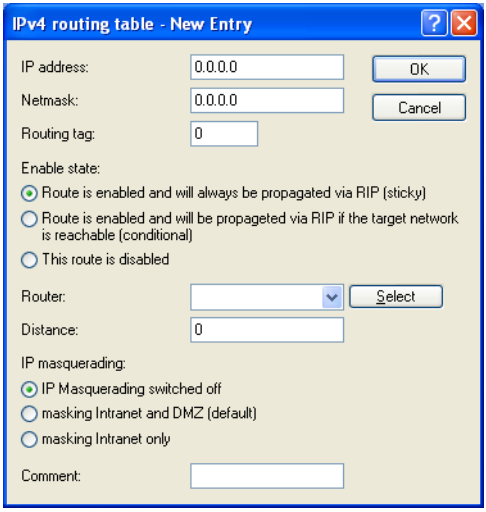
In ‘static routing’, you manually make these entries; they remain unchanged until you either change or delete them yourself. In ‘dynamic routing’, the routers discover existing routes by exchanging data between themselves, then continuously and automatically update this information. The IP router uses the static and the dynamic routing table when the IP Routing Information Protocol (RIP) is activated.

The IP routing table also determines the length of a route's path, so that the router can select the most suitable route—from among several existing routes—to the destination. The default setting for the distance to another router is 0, indicating that the other router can be reached directly. All devices that can be reached locally—including other routers in the same LAN or workstation computers connected via proxy ARP—are assigned the distance 0. The ‘quality level’ of this route is reduced if the entry addressed has a higher distance (up to 14). ‘Unfavorable’ routes with higher distance values are used if no other route to a particular remote station can be found.

Configuring the Routing Table

To access the routing table for editing:

☐ Navigate to the following dialog:`Configuration : IP Router: Routing`, and click ‘IPv4 routing table...’.



In the Routing table, you can edit an existing entry by selecting it then clicking ‘Edit...’ or create a new entry by clicking ‘Add...’

A routing table entry can include settings for the following parameters:

- IP addresses and Netmask:
  This is the address of the destination network to which data packets may be sent and its associated network mask. The router uses the network mask and the destination IP address of the incoming data packets to check whether the packet belongs to the destination network.

  The route with the IP address '255.255.255.255' and the network mask '0.0.0.0' is the default route. All data packets that cannot be routed by other routing entries are sent over this route.

- Routing tag:
  This permits more precise control of the selection of the target route. The target IP address for the selected route is detected, as well as other information that is joined to the data packets by the firewall. The routing tag ’0’ indicates the routing entry is valid for all packets.

- Enable state:
  Indicates if the route is enabled or disabled, and how the route will be propagated for RIP. For enabled networks, RIP propagation can be either:
  – ‘Sticky’: always propagated
  – ‘Conditional’: propagated exclusively if the target network is reachable
  – ‘Off’: never propagated
- Router:
  The router transmits the appropriate data packets to the IP address and network mask to this remote station.
  – If the remote station is a router in another network or an individual workstation computer, this is the name of the remote station.
  – If the router on the network cannot address the remote station itself, then the IP address of another router which knows the path to the destination network is entered.

  The router name indicates what should happen with the data packets that match the IP address and network mask:
  – Routes with the entry '0.0.0.0' identify exclusion routes. Data packets for this ‘zero route’ are rejected and are not routed any further. That way routes which are inaccessible on the Internet (private address spaces, e.g., '10.0.0.0'), for example, are excluded from transmission.
  – If an IP address is input as router name, this is a locally available router, which is responsible for transfer of the relevant data packets.
- Distance:
  The number of routers between this router and the destination router. This value is often equated with the cost of the transmission and used to distinguish between inexpensive and expensive call paths for wide-area connections. The distance values entered are propagated as follows:
  – All networks which can be reached while a connection exists to a destination network are propagated with a distance of 1.
  – All non-connected networks are propagated with the distance entered in the routing table (but with a minimum distance of 2) as long as a free transmitting channel is still available.

  - The remaining networks are propagated with a distance of 16 (= unreachable) if there are no longer any channels available.
  - Remote stations connected using proxy ARP are an exception to this. These ‘proxy hosts’ are not propagated.

- Masquerading:
  IP masquerading can be used to hide a logical IP network behind a single address – namely, that of the router. For example, if you have Internet access, you can use this functionality to connect your entire network to the Internet. When IP Masquerading is turned on, its scope can extend to:
  - Interfaces (Intranet) and DMZ
  - Intranet only

10.2.2 Policy Based Routing

Policy-based routing uses other criteria along with the destination IP address to define the destination route (meaning the remote device that is to be used to transfer the data). Additional information can be employed—including the service or the protocol used, sender addresses or the destination for the data packets—for selection of the destination route. Policy-based routing can be used to achieve a more finely controlled routing behavior, as in the following application scenarios:

- The LAN's entire Internet traffic is diverted to a proxy without entering the proxy address into the browsers. As the users do not notice the proxy routing, the scenario is named ‘transparent’ proxy:

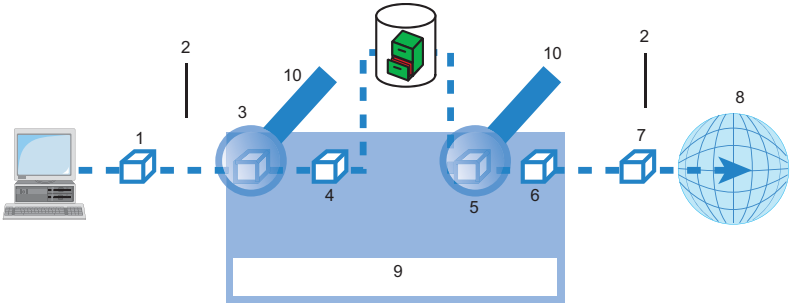


Figure 109:Policy-based routing

1: Data packet with destination address in Internet			
2: Firewall			
3: Source: Local network all port 80			
4: Data packet with destination address and IP routing tag ‘1’			
5: Source: Proxy destination: all port 80			
6: Data packet with destination address and IP			
7: Data packet routed to the Internet			
8: Internet			
9: Table: Extract of IP routing tables:			
IP Address	Net mask	RT tag	Router
255.255.255.255	0.0.0.0	1	Proxy
255.255.255.255	0.0.0.0	0	Internet
10: Firewall rules			

- With load balancing, the data traffic for selected protocols is diverted over a specified DSL port that uses an additional external ADSL modem.
- A server in the local network is supposed to be accessible exclusively from the WAN via a fixed IP address; this is routed via a specified WAN interface.

Appropriate settings can be made causing the firewall to select channels according to information other than just the destination IP address. These entries are supplemented with a special routing tag that is used to control the channel selection with the routing table. For example, a rule can add the routing tag '2' to all data traffic for a local group of computers (defined by an IP address range). Alternatively, data traffic based on specified protocols can be configured to receive a different supplementary routing tag.

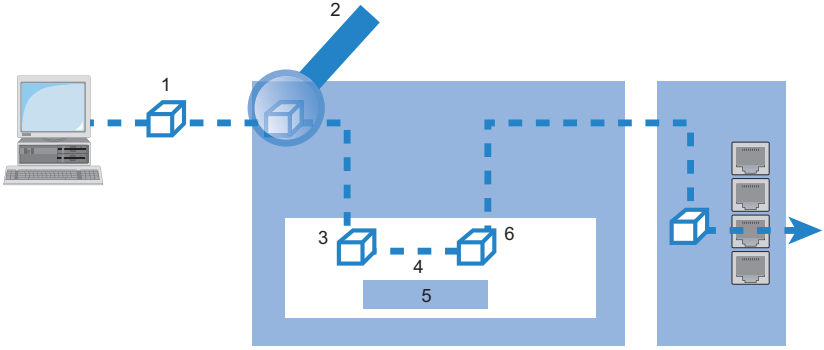


Figure 110:Application of policy-based routing with load balancing

1: Data packet with IP destination address
2: Firewall rules
3: Data packet with IP destination address, IP routing tag
4: IP router
5: Chart:
IP routing table IP address -> Routing tag ->Remote station
6: Data packet with IP destination address, IP routing tag, and DSL port

- When establishing a connection, the firewall initially checks if the packets for transmission fit a rule that applies a routing tag. If so, the routing tag is entered into the data packet.
- The IP routing table combines the routing tag and destination IP address to determine the appropriate remote station. The IP routing table is processed from top down in the usual fashion.
- If an entry is found that corresponds to the remote network, then the router checks the routing tag. The required remote station can be found with the help of the appropriate routing tag.

Note: If the routing tag has a value of ‘0’ (default) then the routing entry applies to all packets.

- Internal services implicitly use the default tag. Using the appropriate firewall rule, you can configure the transfer all services from all source stations to all destination stations with routing tag ‘1’.
- Routing tags and RIP: The routing tag is also transmitted in RIP packets for processing upon reception, so that, for example, the distance setting of the proper route can be changed.

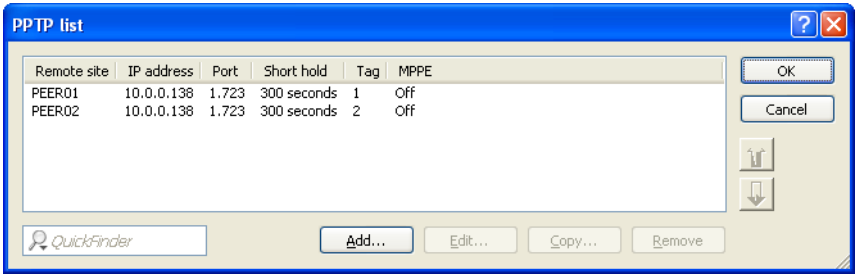
Routing Tags for PPTP Connections

Routing tags are used by the OpenBAT device to evaluate criteria relevant to the selection of the target route, in addition to the IP address. In general, routing tags are added to the data packets using special firewall rules. However, in some cases, it is desirable to assign the tags directly.

In the PPTP table, a routing tag can be entered in addition to the IP address of the PPTP server. Using this routing tag, two or more DSL modems that use a single IP address can be operated on different DSL ports. To configure the PPTP list:

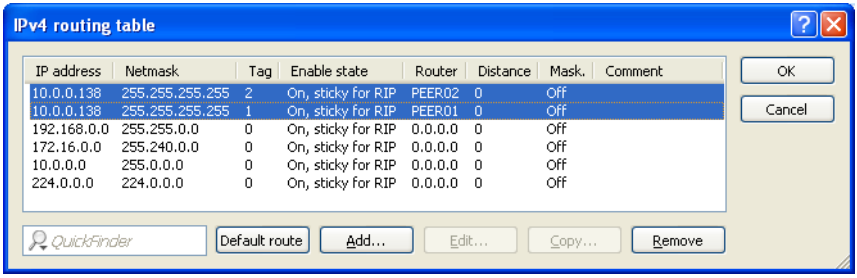
☐ Use the `Configuration : Communication : Protocols` dialog to open the "PPTP list" and click "Add".

☐ Set up the PPT peers as instructed on page 574 „Configuring Remote Stations“. Give each remote terminal its own routing tag.



In the IP routing table, two appropriately tagged routes are required. To access the IP routing table:

☐ In the `Configuration : IP Router : Routing` dialog, click "IPv4 routing table".



10.2.3 Local Routing

When a workstation within a local network attempts to transmit a data packet to an IP address that is outside its own LAN, it searches for a router. Typically, the router is identified in the workstation configuration by means of an entry identifying it as a standard router or standard gateway. It is frequently the case that the workstation can be configured with just a single default router—which is presumed to be able to reach all IP addresses that are unknown to the workstation—even in cases where there are multiple routers on the local network. Sometimes the default router is unable to reach the destination network itself, but does know of another router that can find this destination.

ICMP Redirects

In this case, the designated router sends the computer a response—known as an ICMP redirect—that identifies the address of the router that knows the route to the destination network. The workstation computer then accepts this address and sends the data packet straight to the other router.

However, some workstations cannot handle ICMP redirects. To deliver data packets in this case, use local routing. By means of local routing, the default router sends the data packet directly to other routers. Local routing is enabled by disabling the ICMP redirect function:

☐ Open the `Configuration : IP Router : General` dialog and de-select ‘Send ICMP redirects’.

Note: Local routing should be used sparingly, because it doubles the network load of transmitted data packets. Data is first sent by a workstation to the default router, which then re-sends the data over the same network to a second router that can forward it to the target remote network.

10.2.4 Dynamic Routing with IP RIP

In addition to the static routing table, Hirschmann routers also include a dynamic routing table. Unlike the static table, you do not propagate this yourself, but instead leave this task to the router. The router uses the Routing Information Protocol (RIP) for this purpose. Devices that support RIP use this protocol to exchange information on the available routes.

Information Propagated by IP RIP

A router uses IP RIP to inform other network routers of the routes entered in its own static routing table, except for the following routes:

- Rejected routes with the '0.0.0.0' router setting
- Routes referring to other routers in the local network
- Routes linking individual computers to the LAN by proxy ARP

Although the entries in the static routing table are set manually, both this information—and the transmitted RIP packets based on it—changes according to the connection status of the router:

- If the router has established a connection to a remote station, it propagates all the networks that can be reached via this route in the RIPs with the distance '1'. This informs other routers in the LAN that a connection to the remote station has been established on this router. This means that other routers do not need to establish additional connections, thereby reducing connection costs.
- If this router cannot establish a connection to another remote station, all other routes are propagated with the distance '16' in the RIP. The '16' indicates the route is not currently available.

Information Received in IP RIP Packets

When the router receives IP RIP packets, it incorporates them in its dynamic routing table, which looks something like this:

IP address	IP netmask	Time	Distance	Router
192.168.120.0	255.255.255.0	1	2	192.168.110.1
192.168.130.0	255.255.255.0	5	3	192.168.110.2
192.168.140.0	255.255.255.0	1	5	192.168.110.3

Time-Based Structure of the Dynamic Routing Table

Each route entered in the dynamic routing table includes a value for the following fields:

- IP address and IP netmask:
  Together, these identify the destination network.
- Distance:
  Indicates the number of routers between the transmitter and receiver.
- Router:
  identifies the specific router that has revealed the route.
- Time:
  This parameter acts as a multiplier, and indicates how long the route has been in the table. A newly added route is assigned the value of 1 and is automatically incremented when the corresponding amount of time—about 30 seconds—has elapsed. Thus, a value of 5 indicates the entry has existed for about 2.5 minutes, and so on. After about 3.5 minutes, the Distance value is set to 16 (route not reachable). After about 5.5 minutes, the route is deleted from the table.

When the router receives an IP RIP packet, it needs to decide whether or not to add the contained route to its dynamic table, as follows:

- The route is incorporated if it is not yet listed in the table (as long as there is enough space in the table).
- The route exists in the table with a time of '5' or '6'. The new route is then used if it indicates the same or a better distance.
- The route exists in the table with a time of '7' to '10' and thus has the distance '16'. The new route will be used.
- The route exists in the table. The new route comes from the same router that discovered the route, but has a worse distance than the previous entry. When a device reports the degradation of its own static routing table (e.g. releasing a connection increases the distance from 1 to 2), the router adds the poorer entry to its dynamic table.

Note: RIP packets from the WAN will be ignored and will be rejected immediately. RIP packets from the LAN will be evaluated and will not be propagated in the LAN.

The interaction between static and dynamic tables

The router uses the static and dynamic tables to calculate the actual IP routing table it uses to determine the path for data packets. In doing so, it includes the routes from the dynamic table that it did not itself detect—or which indicate a shorter distance than the same route in its own static table—with the routes from its own static table.

Scaling with IP RIP

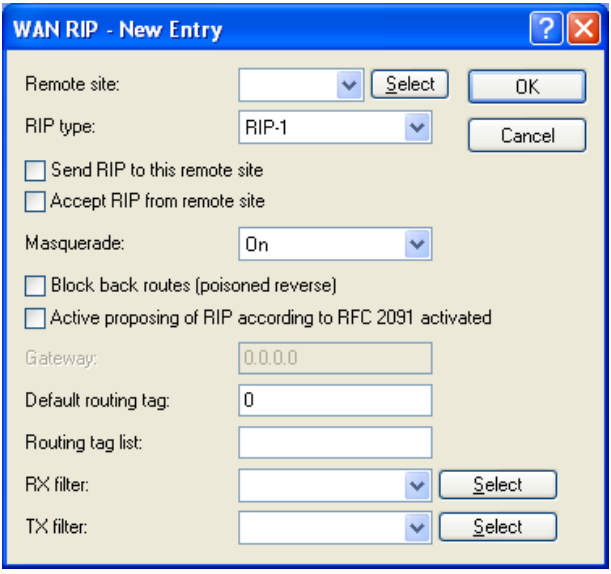
If you use several routers in a local network with IP RIP, you can represent the routers outwardly as a single large router. This procedure is known as ‘scaling’. By constantly exchanging information among the routers, the outwardly projected ‘single router’ theoretically has no limits to the transmission options available to it.

Configuring IP RIP

You can add remote sites to the RIP table, and indicate if the router will send RIP packets to the remote site, or receive RIP packets from the remote site, or both. To configure the RIP table:

☐ Open the `Configuration : IP Router : General` dialog and click ‘WAN RIP...’.

☐ In the ‘WAN RIP’ table, click ‘Add...’ to open the ‘New Entry‘ dialog:



☐ Refer to the topic ‘WAN RIP’ (see on page 640) for a description of this dialog.

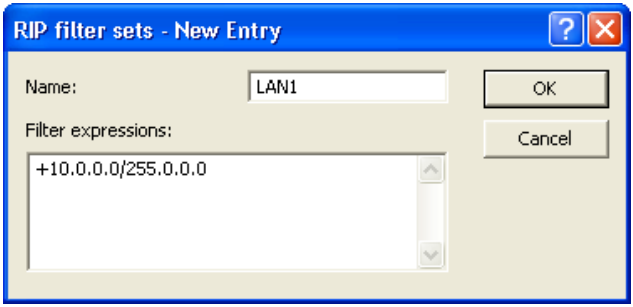
Note: Routers with RIP capabilities dispatch the RIP packets approximately every 30 seconds.The router is set up to send and receive RIPs if it has a unique IP address.The IP RIP module is deselected in the default setting using the IP address xxx.xxx.xxx.254

Configuring the RIP Filter

Routes learned from RIP can be filtered by their routing tag according to the settings for LAN and WAN RIP. Routes can additionally be filtered by specifying network addresses. RIP filters are contained in a central table, and can be applied against entries in the LAN and WAN RIP tables. To create a RIP filter:

☐ Open the `Configuration : IP Router : General` dialog and select ‘RIP filter sets...’.

☐ In the ‘RIP filter sets’ table, click ‘Add...’ to open the New Entry dialog:

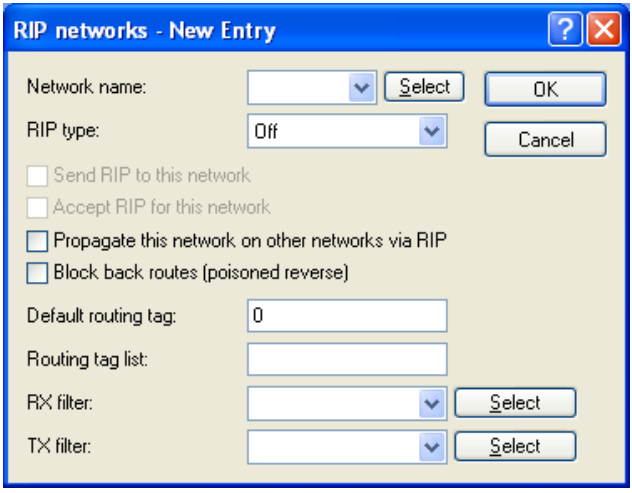


Configure RIP for Separate Networks

It is often not desirable to propagate routing table data equally to all networks. For example, it usually makes little sense to propagate the local route structure via RIP to the DMZ. Similarly, while it may be necessary to propagate the known routes to certain networks, it is not necessary for the router to learn routes from the network (e.g. in the WAN). For these reasons, the router lets you separately configure RIP functionality for every network. To configure RIP for separate networks:

☐ Open the `Configuration : IP Router : General` dialog and select ‘RIP networks...’.

☐ In the ‘RIP networks’ table, click ‘Add...’ to open the New Entry dialog:



Timer Settings

The Routing Information Protocol (RIP) regularly provides neighboring routers with updates on the available networks and the associated metrics (hops). RIP uses various timers to control the exchange of routing information. These timers include the following:

- Update Delay
- Update

They can be viewed and configured in WEBconfig in the Hirschmann Menu Tree at

`Setup : IP Router : RIP : Preferences`

Triggered Update in the LAN

With a triggered update, changes to the metrics are immediately reported to the neighboring router. The system does not wait until the next regular update. An update delay helps prevent imperfect configurations from causing excessive update messages.

- Update delay:
  The delay begins when the routing table, or parts of it, are propagated. While this delay is active, new routing information is accepted and entered into the table, but it is not reported any further. The router actively reports its current entries after expiration of this delay.

  This setting establishes the upper limit for the delay. The actual delay is a random value between one second and this setting.

Triggered Update in the WAN

WAN bandwidth limitations may make regular updates every 30 seconds undesirable. For this reason, RFC 2091 requires that routes are transmitted to the WAN when the connection is established. After this, just updates are transmitted.

Because updates are explicitly requested, broadcasts or multicasts should not be used for delivering RIP messages. Instead, the subsidiary device needs to be statically configured with the IP address of the next available router at the central location. Due to these requests, the central router knows which subsidiary routers it has received update requests from; it sends any messages on route changes directly to the subsidiary device.

To configure a triggered update for a WAN:

- ☐ Navigate to the following dialog:`Configuration : IP Router:General` dialog and click ‘WAN RIP...’.
- ☐ In the ‘WAN RIP’ table, select the WAN and click ‘Edit...’.
- ☐ In the ‘Edit Entry’ dialog, select ‘Active proposing of RIP according to RFC 2091 activated’, then input the target Gateway address.

Poisoned Reverse

Poisoned reverse stops the formation of routing loops. An update is sent back to the router that propagated the route to inform it that the network is unreachable at the associated interface.

This has a significant disadvantage over WAN connections: The central location transmits a high number of routes, which then suffer from route poisoning, leading to a heavy load on the bandwidth. For this reason, poisoned reverse can be manually activated for a LAN/WAN interface.

To enable poison reverse for a LAN:

- ☐ Open the `Configuration : IP Router : General` dialog and select ‘RIP networks...’.
- ☐ In the ‘RIP networks’ table, select the network and click ‘Edit...’.
- ☐ In the ‘Edit Entry’ dialog, select ‘Block back routes (poison reverse)’.

To enable poison reverse for a WAN:

- ☐ Navigate to the following dialog:`Configuration : IP Router :General` dialog and click ‘WAN RIP...’.
- ☐ In the ‘WAN RIP’ table, select the WAN and click ‘Edit...’.
- ☐ In the ‘Edit Entry’ dialog, select ‘Block back routes (poison reverse)’.

Static Routes for Constant Propagation

Routers use RIP to propagate both dynamic routes and statically configured routes as well. Some of these static routes may not be constantly available, for example, when an Internet connection or dial-up access is temporarily unavailable. For a static route, the ‘Active’ setting in the routing table indicates if it should be propagated constantly or exclusively when it is actually reachable. You can edit this setting using WEBconfig in the Hirschmann Menu Tree at:

`Setup : IP-Router : IP-Routing-Table`

10.2.5 SYN/ACK Speedup

SYN/ACK speedup is used to accelerate IP data traffic. The IP check characters (SYN for synchronization and ACK for acknowledge) are given preference within the transmission buffer over simple data packets. Check characters are not delayed in the transmission queue causing the remote station to stop sending data.

The effect of SYN/ACK speedup is most apparent for fast connections (e.g. ADSL) when data quantities are simultaneously transferred in both directions at high speed.

SYN/ACK speedup is enabled by default.

Disabling SYN/ACK Speedup

SYN/ACK speedup changes the order of packet delivery. In some cases, where a protocol assumes a certain packet delivery sequence, this may be undesirable. In this case the SYN/ACK speedup can be deactivated.

To de-activate SYN/ACK speedup:

☐ Open the `Configuration : IP Router : General` dialog and de-select ‘Pass on TCP SYN and ACK packets preferentially’.

10.3 Advanced Routing and Forwarding

10.3.1 Introduction

For some applications, it may be desirable to operate more than one intranet and one DMZ with a OpenBAT device—for example, in order to provide multiple IP networks with Internet access via a central router. OpenBAT devices support up to 64 different IP networks.

Various scenarios are possible when operating multiple IP networks:

- One network per interface
- Multiple networks per interface
- Multiple VLANs per interface; one or more networks per VLAN (a combination of the first two scenarios)

The implementation of these scenarios is facilitated by advanced routing and forwarding (ARF), which provides very flexible options in the definition of IP networks and the assignment of these networks to the interfaces. The diagram below illustrates the network/interface assignment at various levels. The configuration options applied here are described in the following chapters:

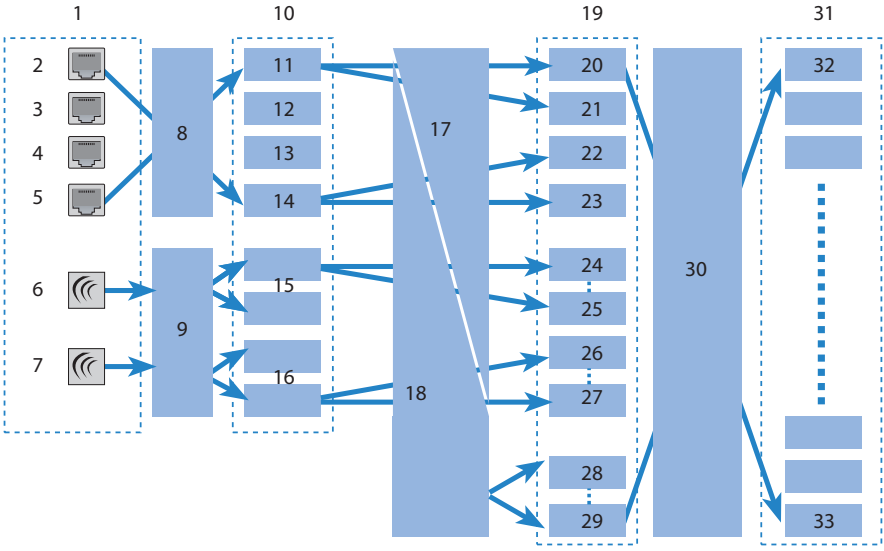


Figure 111:Network/interface assignment at various levels

1: Physical interfaces	10: Logical interfaces	19: Logical interfaces with VLAN tags, bridge groups	30: Advanced Routing and Forwarding
2: ETH - 1	11: LAN - 1	20: LAN-1, VLAN ID 1	31: IP networks
3: ETH - 2	12: LAN - 2	21: LAN-1, VLAN ID 5	32: Network 1
4: ETH - 3	13: LAN - 3	22: LAN-4, VLAN ID 6	33: Network 64
5: ETH - 4	14: LAN - 4	23: LAN-4, VLAN ID 9	
6: WLAN - 1	15: WLAN-1-1 to P2P-1-16	24: WLAN-1-1, VLAN ID 10	
7: WLAN - 2	16: WLAN-2-1 to P2P-2-16	25: P2P-1-6, VLAN ID 18	
8: Ethernet port mapping	17: VLANs	26: WLAN-1-1, VLAN ID 19	
9: Multi-SSID, P2P	18: LAN bridge	27: P2P-1-6, VLAN ID 25	
		28: BRG-1	
		29: BRG-8	

The assignment of IP networks to interfaces proceeds as follows:

- Different models of the OpenBAT devices present varying numbers of physical interfaces—i.e. Ethernet (LAN) ports or WLAN radio modules.
- Each logical interface is assigned to a physical interface:
  - For Ethernet ports, port mapping assigns the physical ETH-1 through ETH-4 ports to the logical LAN-1 through LAN-4 ports.

    For some but not all models, the number of logical LAN interfaces corresponds to the number of physically available Ethernet ports.
  - For WLAN modules, the establishment of point-to-point connections (P2P), or the use of Multi-SSID—or both—can mean that multiple WLAN interfaces are assigned to each physical WLAN module. This can include up to eight WLAN networks and up to six P2P connections for each physical WLAN module.
- These logical interfaces are further specified and grouped in the next stage:
  - For devices supporting VLAN, multiple VLANs can be defined for each logical interface simply by using VLAN-IDs. Although the data traffic for the various VLANs flows via a common logical interface, the VLAN-ID keeps the different VLANs strictly separated. From the perspective of the OpenBAT device, the VLANs are completely separate interfaces. This means that a single logical interface becomes multiple logical interfaces for the OpenBAT device, and each of these interfaces can be addressed individually.
  - For devices with WLAN modules, the individual logical interfaces can be grouped together. This is handled by the LAN bridge which regulates data transfer between the LAN and WLAN interfaces. The formation of bridge groups (BRG) allows multiple logical interfaces to be addresses at once; they appear as a single interface to the OpenBAT device—in effect achieving the opposite of the VLAN method.
- In the final stage, the ARF forms a connection between the logical interfaces with VLAN tags and the bridge groups on the one side, and the IP networks on the other. For this reason, an IP network is configured with a reference to a logical network (with VLAN-ID, if applicable) or to a bridge group. Furthermore, an interface tag can be set for each IP network, by means of which the IP network can be separated from other networks without having to use firewall rules.

The definition of routing tags for IP networks as described above is one of the main advantages of ARF. This option allows "virtual routers" to be implemented. A virtual router takes up only a portion of the routing table by using interface tags for an IP-network, and therefore configures routing individually for that particular IP-network. This method allows, for example, several default routes to be defined in the routing table, each of which is given a routing tag. Virtual routers in the IP networks use the tags to select the default route that applies to the IP network with the appropriate interface tag. The separation of IP networks via virtual routers even permits multiple IP networks with one and the same address range to be operated in parallel in just one OpenBAT device without conflict.

One example: Consider the case of an office building that houses several different companies, which need to be connected to the Internet via a central OpenBAT device, even though each of these companies has its own Internet provider. All of the companies want to use the popular IP network '10.0.0.0' with the netmask '255.255.255.0'. To implement these requirements, each company is given an IP network '10.0.0.0/255.255.255.0' with a unique name and a unique interface tag. In the routing table, a default route with the corresponding routing tag is created for each Internet provider. This allows the clients in the different company networks, all of which use the same IP addresses, to access the Internet via their own provider. Employing VLANs enables logical networks to be separated from one another even though they use the same physical medium (Ethernet).

Routing Tags Versus Interface Tags

Routing tags (assigned by the firewall) and interface tags (defined by the IP networks) have a great deal in common, but also some significant differences:

- The router interprets both tags in the same way. Packets with the interface tag '2' are valid for routes with the routing tag set to '2' in the routing table (and all routes with the default route tag '0'). The same routes apply for packets which the firewall has assigned with the routing tag '2'. Thus the interface tag is used in the same way as a routing tag.
- Interface tags have the additional ability to delimit the visibility (or accessibility) between different networks:
  - In principle, networks that are visible to one another, and thus able to interconnect, are those networks that share the same interface tag.
  - Networks with the interface tag '0' have a special significance; they are in effect supervisor networks. The networks can see all of the other networks and can connect to them. Networks with an interface tag not equal to '0' cannot make connections to supervisor networks.
  - Networks of the DMZ type can be seen by all other networks independently of their interface tag—which makes sense, because the DMZ often contains servers that are open to the public, like web servers etc. The DMZ-networks exclusively see networks with the same interface tag (and of course all other DMZ-networks).
  - Networks of the DMZ type with the interface tag '0' have a special significance: As ‘supervisor networks’ they can see all other networks, and they are also visible to all other networks.

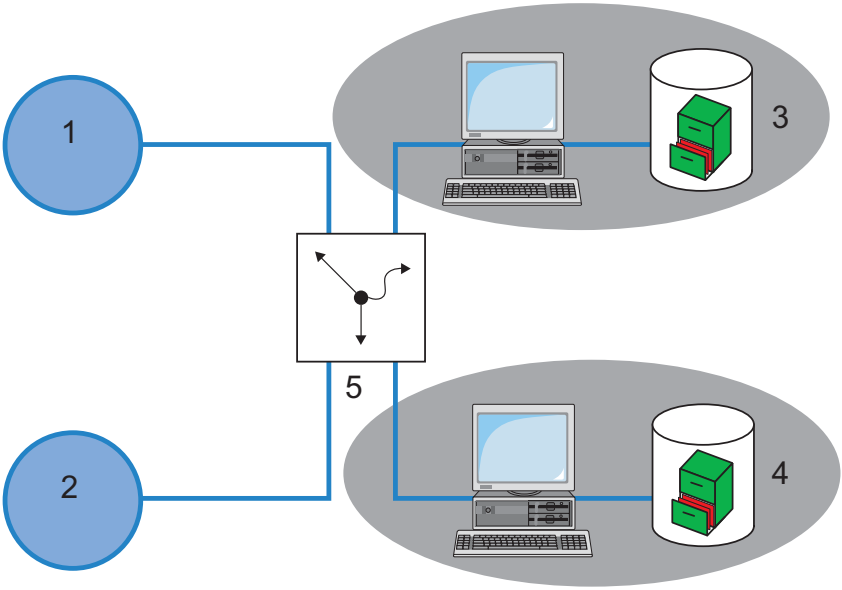


Figure 112:Creating a default route with the corresponding routing tag in the routing table

1: Provider A			
2: Provider B			
3: IP network Company A 10.0.0.0/255.255.255.0, interface tag 1			
4: IP network Company B 10.0.0.0/255.255.255.0, interface tag 2			
5: Routing table:			
IP address	Netmask	Interface tag	Router
255,255,255,255	0.0.0.0	1	Provider A
255,255,255,255	0.0.0.0	2	Provider B

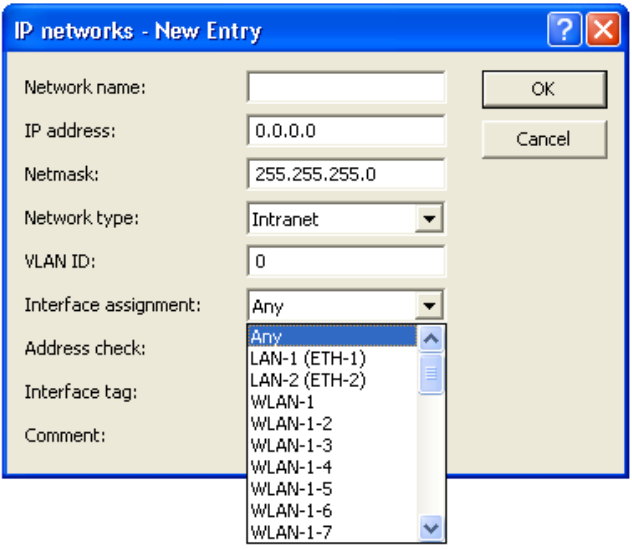
Note: For cases which do not allow IP addresses to be uniquely assigned by interface tags, ARF can be supported by firewall rules. In the above example, this would be the case if each of the networks were to support a public web or mail server, all of which use the same IP address.

10.3.2 Definition of networks and Assignment of Interfaces

When defining a network, the first setting is for the IP-address, which is to be valid for a certain local interface on the OpenBAT device. "Local interfaces" are logical interfaces that are assigned either to a physical Ethernet port (LAN) or a wireless port (WLAN). It is possible for several networks to be active on one interface in order to implement the scenarios above. Conversely, a network can also be active on multiple interfaces (via bridge groups or with the interface assignment "Any"). To define a new network:

☐ Navigate to the following dialog:`Configuration : IPv4 : General` dialog and click "IP networks".

☐ Click "Add" to open the following dialog:



In this dialog, enter values for at least the following fields:

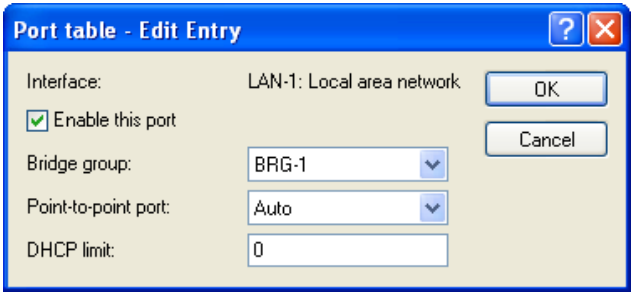
- Network Name: A unique network name allows the identification of networks in other modules (DHCP server, RIP, NetBIOS, etc.) and enables control over which services are available in which networks.
- IP address and Netmask
- Network type: Intranet or DMZ

10.3.3 Assigning Logical Interfaces to Bridge Groups

Particular properties of the logical interfaces are defined in the port table. To configure an interface:

☐ Navigate to the following dialog:`Configuration :Interfaces : LAN` dialog and click "Port table".

☐ Select an interface to open the port table configuration dialog:



In this dialog, enter values for the following fields:

- Enable this port:
  This option activates or deactivates the logical interfaces.
- Bridge group:
  Assigns the logical interface to a bridge group to enable bridging from/to this logical interface via the LAN bridge. If assigned to a common bridge group, several logical interfaces can be addressed at once and they appear to the OpenBAT device to be a single interface. This can then be used for ARF.

  If you remove the interface from all bridge groups via the setting "none," then there is no transmission via the LAN bridge between LAN and WLAN (isolated mode). In this setting, a data transfer between LAN and WLAN for this interface is possible only via the router.

- Point-to-point port:
  Sets the priority for the logical interface when the spanning-tree protocol is enabled. If multiple connections are available, the interface with the highest priority is used. The smaller the value, the higher the priority. If priorities are the same then the interface with lower transmission fees is used or, alternatively, the interface that appears in the highest position in the table.
- DHCP limit:
  Number of clients that can be handled by DHCP. If the limit is exceeded, the oldest entry is dropped. This feature can be used in combination with the protocol filter table to limit access to just one logical interface.

10.3.4 Interface Tags for Remote Sites

By defining interface tags, you can configure virtual routers to be used as part of ARF in a way that uses just a part of the overall routing table. For inbound data packets from the WAN, the assignment of interface tags can be regulated in several different ways, including:

- appropriate firewall rules that capture data packets from particular remote sites, IP addresses, or ports
- entries in the routing table
- the explicit assignment of tags to remote sites

The assignment of tags to the remote sites to separate ARF networks can also be conveniently used for packets received at the WAN-side (which by default contain Tag 0). Without controlling the assignment of tags explicitly with the firewall, the virtual router can be identified directly from the remote site or source route by the form of the interface tag. Inbound and outbound communication can thus be easily divided bi-directionally between virtual routers.

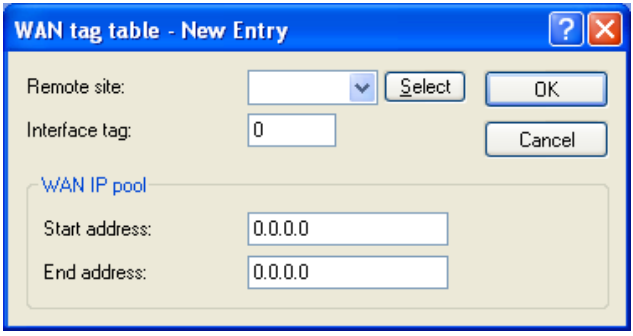
Note: The interface tags determined via the tag table, on the basis of the routing table, can be overwritten with an appropriate entry in the firewall.

Assigning Interface Tags in the WAN Tag Table

To access the dialog where you can add interface tags using the WAN tag table:

☐ Open `Configuration : Communication : Remote Sites` and click 'WAN tag table...'.

☐ In the 'WAN tag table' click 'Add...' to open the 'New Entry' dialog.



WAN Tag Generation

WAN tag generation defines the source for the assignment of interface tags. Besides assignment via the firewall or direct assignment via the tag table, the interface tag can also be selected based on the source route in the effective routing table (static routing entries plus routes learned via RIP). The router compares the source IP and the name of the remote site used to establish the IP connection to the routing information. The routing tag of this source route is assigned for further processing to the packets received at the WAN-side of this connection. If the effective routing table contains more than one entry for a remote site with the same network, the smallest tag is used.

For example, the following ARF networks have been defined:

Network	IP address	Routing tag	Port
PRIVATE	192.168.1.1/24	1	LAN-1:
FACTORY	192.168.10.1/24	10	LAN-2

PRIVATE is to be limited to Internet access; FACTORY is to be limited to the remote site FACTORY. The corresponding effective routing table appears as follows:

IP address	IP netmask	Routing tag	Remote site	Distance	Masking
192.168.10.0	255.255.255.0	10	FACTORY	0	No
255,255,255,255	0.0.0.0	1	INTERNET	0	No

- Data packet coming from network 192.168.10.x: Tag = 10
- Data packet coming from network 192.168.1.x: Tag = 1
- Data packet coming from any other network: Tag = 0

Possible values:

- Manual: With this setting, the interface tags are determined solely by an entry in the tag table. The routing table has no significance in the assignment of interface tags.
- Auto: With this setting, the interface tags are determined initially by an entry in the tag table. If no matching entry is located there, the tag is determined based on the routing table.

Note: The interface tags determined via the tag table and on the basis of the routing table can be overwritten with an appropriate entry in the firewall.

10.3.5 Virtual Routers

By means of interface-dependent filtering, in combination with policy-based routing, virtual routers can be defined for every interface. For example:

Two separate IP networks are used by the Development and Sales departments. Both networks are connected to different switch ports although they use the same network "10.1.1.0/255.255.255.0". Sales should be restricted to accessing the Internet, whereas Development should also have access to a partner company's network ('192.168.1.0/255.255.255.0').

The result is the following routing table (where the Development department has tag 2, Sales has tag 1):

IP address	IP netmask	Rtg tag	Peer or IP	Distance	Masking	Enabled
192.168.1.0	255.255.255.0	2	PARTNER	0	No	Yes
192.168.0.0	255.255.0.0	0	0.0.0.0	0	No	Yes
255,255,255,255	0.0.0.0	2	INTERNET	2	Yes	Yes
255,255,255,255	0.0.0.0	1	INTERNET	2	Yes	Yes

If Development and Sales were in IP networks with different address ranges, then it would be possible to assign the routing tags with firewall rules. But because both departments are in the same IP network, the only available method of assignment is with network names.

Tag assignment can be carried out directly in the network definition:

"Name"	IP address	Netmask	VLAN-ID	Interface	Source check	Type	Rtg tag
DEVELOPMENT	10.1.1.1	255.255.255.0	0	LAN-1:	strict	Intranet	2
Sales	10.1.1.1	255.255.255.0	0	LAN-2	strict	Intranet	1

Alternatively the assignment of tags can be carried out with a combination of network definitions and firewall rules. The networks are defined as follows:

"Name"	IP address	Netmask	VLAN-ID	Interface	Source check	Type	Rtg tag
DEVELOPMENT	10.1.1.1	255.255.255.0	0	LAN-1:	strict	Intranet	0
Sales	10.1.1.1	255.255.255.0	0	LAN-2	strict	Intranet	0

Routing tags can be used to define the following firewall rules:

"Name"	Protocol	Source	Destination	Action	Linked	Prio	(...)	Rtg tag
DEVELOPMENT	ANY	%Ldevelopment	ANYHOST	%a	Yes	255		2
Sales	ANY	%Lsales	ANYHOST	%a	Yes	255		1

Set these rules to the maximum priority (255), so that they are checked first. Because filtering is still possible by services, set the option "Linked" in the firewall rule.

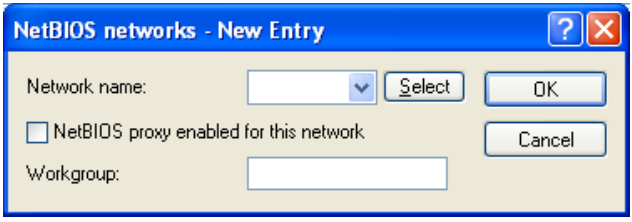
10.3.6 NetBIOS Proxy

Configure the behavior of the NetBIOS proxy separately for each network for which it is relevant—for example, the NetBIOS proxy normally is not active within the DMZ.

To configure the NetBIOS proxy:

☐ Navigate to the following dialog:`Configuration : NetBIOS : General` dialog and click "NetBIOS networks".

☐ Click "Add" to open the following dialog:



In this dialog, enter values for the following fields:

- network name:
  Name of the network for which the NetBIOS proxy is to be activated.
- NetBIOS proxy enabled for this network:
  Select this to activate the NetBIOS-proxy for the selected network.
- Workgroup:
  Enter the name of the workgroup or domain used by the network clients. If multiple workgroups exist within the network, enter just one workgroup name.

Note: By default, networks 'Intranet' and 'DMZ' are entered into the list of NetBIOS networks. The NetBIOS proxy is activated for intranet and deactivated for DMZ.

As soon as a network is assigned to an interface tag, then the names (hosts and groups) that are visible from this network are those in a network with the same tag, or which are accessible via a suitably tagged (with the same tag) WAN route. An untagged network sees all names. Similarly, all names learned from untagged networks are visible to all networks.

The DNS server considers the interface tags when resolving names, i.e. the names resolved by DNS are those learned from a network with the same tag. The special role played by untagged networks applies here too.

The workgroup/domain enables networks to be scanned for NetBIOS names when a device is started. The workgroup is different for every network and has to be defined everywhere. In networks without domains, the name of the largest workgroup should be defined here.

10.4 Configuring Remote Stations

Remote stations are configured in two tables:

- In the remote site (peer) table all information is input that applies exclusively to a single remote station.
- Parameters for the lower protocol levels (below IP or IPX) are defined in the communication layer table.

Note: The configuration of the authentication (protocol, user name, password) is not covered in this section. Information on authentication is contained in the section ‘Establishing connection with PPP’ (see on page 600).

10.4.1 Remote Site (Peer) List

The available remote stations are created in the peer list with a suitable name and additional parameters. For every WAN interface exists a separate peer list. There are two separate input dialogs for the peer list: one for DSL connections, one for serial connections. To add new remote stations to the peer list:

☐ Navigate to the following dialog:`Configuration : Communication Remote Sites` and click either the button

  – "Remote sites (DSL)..." or

  – "Remote sites (Serial)..."

The following parameters can be configured for each remote station:

Preferences	Used where (in which peer list)	Description
Name	DSL/Serial	Enter the name of the remote station.
Phone number	Serial	The dialup telephone number for the remote station. A number is required if phone calls need to be made to the remote station. This field can remain empty if just incoming calls should be accepted. Several phone numbers for the same remote station can be entered in the RoundRobin list.
Short hold time	DSL/Serial	The time, in seconds, after which the connection should be closed if no data has been transferred.
Short hold time (bundle)	Serial	If a second channel has been opened to the remote station (bundling), it will be closed after the time specified here if no data has been transferred.
Access concentrator	DSL	Used, with the Service parameter, to identify your Internet provider. Contact your Internet provider for this information.
Service	DSL	Used, with the Access concentrator parameter, to identify your Internet provider. Contact your Internet provider for this information.
Layer name	DSL/Serial	Select the layer name for the connection. The configuration of this layer is described in the following section (see on page 576).
MAC address type	DSL	Select which MAC address should be used: ▶ Local: Additional virtual addresses are generated for each WAN connection, based on the device MAC address. ▶ Global: The device MAC address will be used for all connections. ▶ User-defined: Input a MAC address for the remote gateway in the “MAC address” field.
MAC address	DSL	The MAC address for user defined types.

Preferences	Used where (in which peer list)	Description
VLAN ID	DSL	The VLAN identifier if the remote station connection is part of a VLAN.
Automatic callback	Serial	When automatic callback is enabled, a call from the remote station will not be accepted, but the remote station will be called back. This is useful to provide a secure connection, and reduce the connect charges for the remote site. **Note:** ▶ If you select the “fast procedure” option, callback may take one or two seconds. However, on the remote device, be sure the remote site supports this option and “wait for callback” is enabled. ▶ Select “Call back the remote site after name verification” to force the remote site to be authenticated before calling back.

When editing the remote site peers list, note the following:

- If a remote site appears on the two lists, the OpenBAT device uses the faster interface to connect to the remote site. The other interface is used as a backup.
- If neither the access concentrator nor the service is specified, the router connects to the first access concentrator that answers the query.

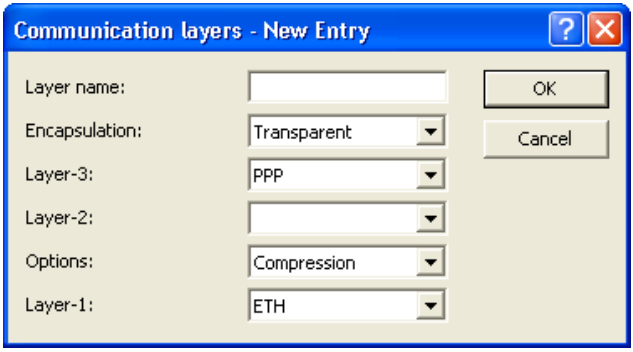
10.4.2 Communication Layers List

A communication layer is a collection of protocol settings that are used when connecting to specific remote stations. By default, the communication layers list includes layer entries with common combinations of protocols. Changes or additions to this list should be made if remote stations are incompatible with all of the existing layer entries.

To access the communication layers list:

☐ Navigate to the following dialog:`Configuration : Communication General` dialog, and click "Communication layers".

☐ Click "Add" to open the following dialog:



A layer entry can contain combinations of the following options.

Note: The available selection possibilities in a given OpenBAT device depend on the device model. Some devices offer the options described below.

Parameter	Description	
Layer name	The layer is selected in the peer list under this name.	
Encapsulation	Additional encapsulations can be set for data packets.	
	Transparent	No additional encapsulations.
	Ethernet	Encapsulation in the form of Ethernet frames.
Layer 3	The following options are available for the switching layer or network layer.	
	Transparent	No additional header is inserted
	PPP	The connection is established according to the PPP protocol (in the synchronous mode, i.e. bit-oriented). The configuration data is taken from the PPP table
	AsyncPPP	Like "PPP" only in asynchronous mode. This means that PPP functions character-oriented.
	... with script	All options can be run with their own script if desired. The script is specified in the script list.
	DHCP	Assignment of the network parameters via DHCP

Parameter	Description	
Layer 2	In this field the upper section of the security layer (Data Link Layer) is configured. The following options are available:	
	Transparent	No additional header is inserted
	PPPoE	The PPP negotiation runs via Ethernet. The PPP packets are encapsulated in Ethernet frames for this purpose. This process is frequently used for DSL connections.
Option	Here you can activate the compression of the data to be transmitted and the bundling of channels. The selected option becomes active when it is supported by both the ports used and the selected Layer-2 and Layer-3 protocols.	
Layer 1	In this field the lower section of the security layer (Data Link Layer) is configured. The following options are available:	
	ETH	Transparent Ethernet as per IEEE 802.3
	Serial	Transmission via the serial interface

10.5 IP Masquerading

One of the most common tasks for a router is to connect LAN workstations to the Internet. For security reasons, hide the IP address of each LAN workstation to the entire internet. IP masquerading can hide the IP addresses of LAN workstations. IP masquerading operates in a router that has been configured with two IP addresses:

- an intranet IP address—typically a private IP address—which the router uses to communicate with computers in the LAN, and
- a public IP address, which the router uses to communicate with remote stations in the Internet

The computers in the LAN use the router as a gateway but are not recognizable themselves. The router divides the intranet from the Internet.

10.5.1 Simple Masquerading

How IP Masquerading Works

Masquerading uses a feature of TCP/IP data transmission—source and destination port numbers—in addition to the source and destination addresses. When the router receives a data packet for transfer, it records the IP address and the sender's port in an internal table. It next assigns the packet the router’s public IP address and a new port number, which could be any number. The router enters this new data in its internal table, and forwards the packet.

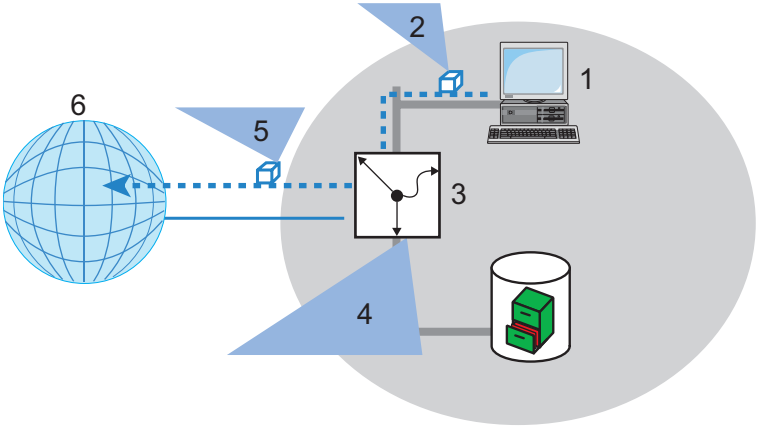


Figure 113:IP masquerading: forwarding data packet with new information

1: Internal workstation: IP address 10.0.0.100
2: Data packet - Source: 10.0.0.100, Target: 80.123.123.123
3: Router - Internal IP address: 10.0.0.1, Public IP address: 80.146.74.146
4: Internal router table entry - Source IP: 10.0.0.100, Port: 3456
5: Data packet - Source: 80.146.74.146, Port 3456, Target: 80.123.123.123
6: Internet

The response to this new packet is now sent to the IP address of the router with the new sender port number. The entry in the internal table allows the router to assign this response to the original sender again:

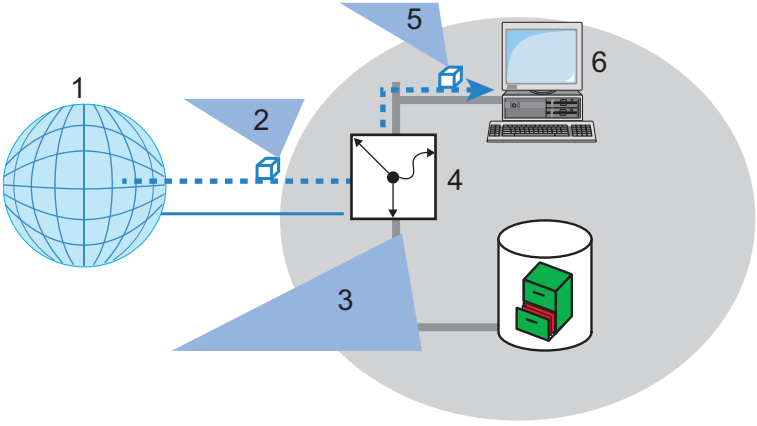


Figure 114:IP masquerading: assigning the response to the original sender

1: Internet
2: Data packet - Source: 80.123.123.123, target: 80.146.74.146
3: Internal router table entry - Source IP: 10.0.0.100, Port: 3456
4: Router - Internal IP address: 10.0.0.1, Public IP address: 80.146.74.146
5: Data packet - Source: 80.123.123.123, target: 10.0.0.100
6: Internal workstation: IP address 10.0.0.100

Protocols that can be Transmitted via IP Masquerading

IP masquerading can transmit IP protocols that are based on TCP, UDP, or ICMP and communicate exclusively through ports. One example of this type of uncomplicated protocol is the one on which the World Wide Web is based: HTTP.

Individual IP protocols do use TCP or UDP, but do not, however communicate exclusively through ports. This type of protocol calls for a corresponding special procedure for IP masquerading. Among the group of protocols supported by IP masquerading in the OpenBAT device are:

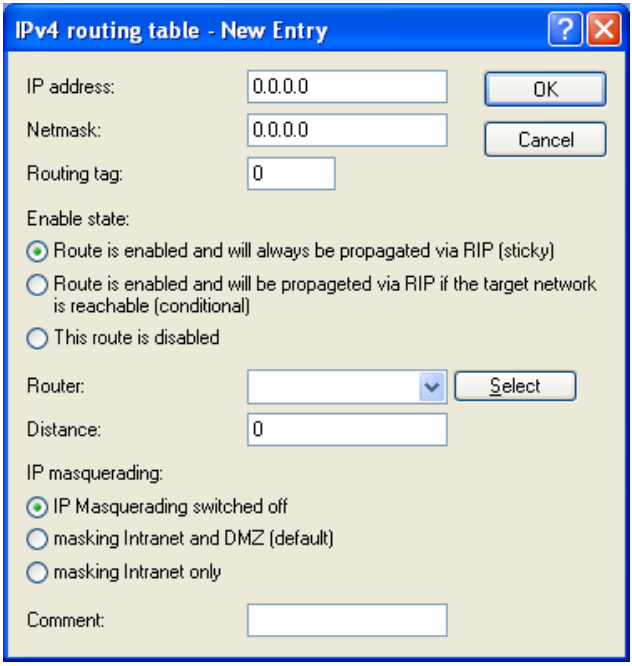
- ftp (using the standard ports)
- H.323 (to the same extent as used by Microsoft Netmeeting)
- Point-to-Point Tunneling Protocol (PPTP)
- Internet Protocol Security (IPSec)
- Internet Relay chat (IRC)

Configuring IP Masquerading

IP Masquerading can be configured for each entry in the routing table:

☐ Open `Configuration : IP Router. Routing` dialog and click ‘IPv4 routing table...’.

☐ Inside the 'IPv4 routing table', select an entry and click 'Edit...', or click 'Add...' for creating a new entry. The following dialog opens:



You can apply IP masquerading to devices in the Intranet, or in both the Intranet and DMZ.

10.5.2 Inverse Masquerading

Simple masquerading hides internal LAN IP addresses behind the public IP address of the router. However, if a certain device on the LAN—for example an ftp server—is supposed to be available to stations on the internet, simple masquerading would also hide its IP address from Internet devices. A connection to this ftp server from the internet is not possible.

To enable the access to such a server (’exposed host’) in the LAN, the IP address of the ftp server needs to be entered with all services that are accessible from outside the LAN. If a remote device sends a packet from the Internet to the ftp server on the LAN, from the point of view of this remote device, the router appears to be the ftp server. The router reads the IP address of the ftp server in the LAN from the entry in the service table. The packet is forwarded to this computer. Packets that come from the ftp server in the LAN (responses from the server) are hidden behind the IP address of the router.

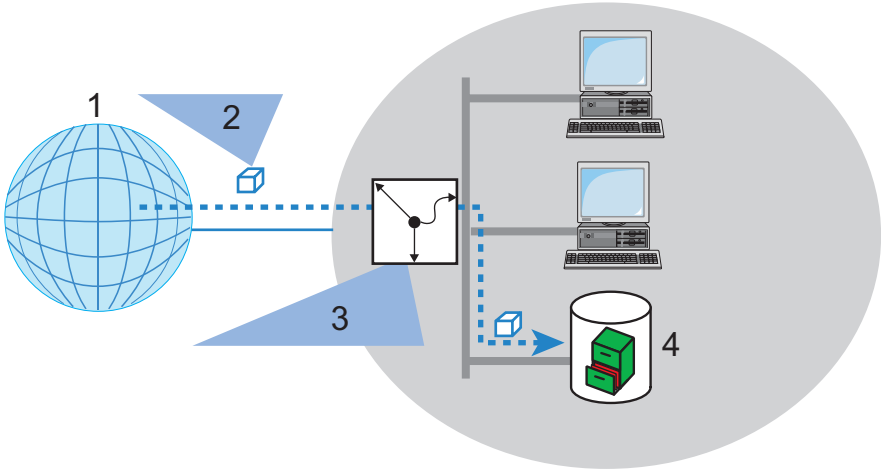


Figure 115:Inverse masquerading

1: Internet
2: Data packet - Source: 80.123.123.123, target: 80.146.74.146, port 21
3: Internal router table entry: Source IP: 10.0.0.100, Port: 3456
4: ftp server - IP address: 10.0.0.10

The difference between simple masquerading and inverse masquerading is that:

- Access to a service (port) in the intranet from outside needs to be defined in advance by specifying a port number. This is achieved by associating the destination port with the intranet address of, for example, the ftp server, in a service table.
- When accessing the Internet from the LAN, the router itself makes the entry in the port and IP address information table.

Note: The table can hold up to 2048 entries, thereby allowing 2048 simultaneous transmissions between the masked and the unmasked network. After a specified period of time, the router assumes that an entry is no longer required and deletes it automatically from the table.

Stateful Inspection and Inverse Masquerading

If the masquerading module exposes a port (for example, packets received on this port are forwarded to a server in the LAN), then this should be implemented with both a Deny All firewall strategy plus an additional entry in the Stateful Inspection firewall, which enables the access by all stations to the respective server.

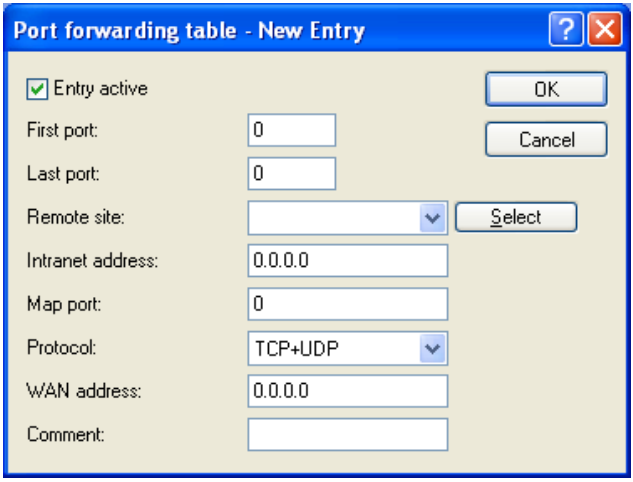
Configuring Port Mapping

On occasion it is desirable for the exposed host not to be contacted over this standard port, e.g. when security reasons demand the use of another port. In this case, both the mapping of ports to an IP address, and the mapping of ports to other ports (port mapping) are necessary. Another use for this port mapping is the assignment of several ports of the WAN to a shared port in the LAN, which can be assigned to different IP addresses.

The configuration of port mapping involves the assignment of a port or port range (first port to last port) to a target IP address from the LAN, and the port (map port) to be used in the LAN. Port mapping is performed in the Port Forwarding table:

☐ Navigate to the following dialog:`Configuration : IP Router : Masq.` and click "Port forwarding table".

☐ Click "Add" to open the following dialog:



Configure the following parameters:

- Entry active:
  Toggles the port mapping entry on and off.
- First port / Last port:
  Defines the port, or range of ports, over which service requests will be received.
- Remote site:
  Select the remote site to which this entry applies. If this is left empty, the entry applies to all remote sites.
- Internet address:
  The intranet (LAN) address of the device providing the service, to which packets will be forwarded.
- Map port:
  The port over which requests will be forwarded. If ‘0’ is entered for the map port, the ports used in the LAN will be the same as those used in the WAN. If a port range is to be mapped, then the map port identifies the first LAN port to be used. For example, mapping the port range '1200' to '1205' to the internal map port '1000' means that the ports 1000 to 1005 will be used for data transfer in the LAN.
  Port mapping is static, meaning that two ports or port ranges cannot be mapped to the same port in a target LAN computer. The same port mapping can be used for different target computers

- Protocol:
  The protocol to which this entry applies.
- WAN address:
  WAN address which applies for this entry. If the device has more than one static IP address, then this allows port forwarding to be limited to certain connections.

10.6 Demilitarized Zone (DMZ)

A demilitarized zone (DMZ) renders certain stations in a network accessible from the Internet. These computers in the DMZ are generally used to offer Internet services such as e-mail or http. The rest of the network should of course be inaccessible from the Internet.

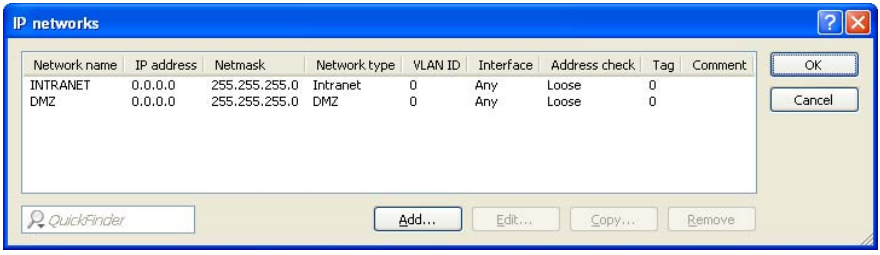
In order to allow this architecture, data traffic between the three zones—Internet, DMZ and LAN—need to be analyzed by a firewall. The firewall's tasks can also be consolidated in a single device (the router). In this design, the router needs to include three separate interfaces that can be monitored independently by the firewall:

- LAN interface
- WAN interface
- DMZ interface

10.6.1 Assigning Networks to the DMZ

In its factory configuration the OpenBAT device is preconfigured with only one logical DMZ network zone. You can access this in LANconfig at the following position. Carry out the following steps to access the present DMZ network zone

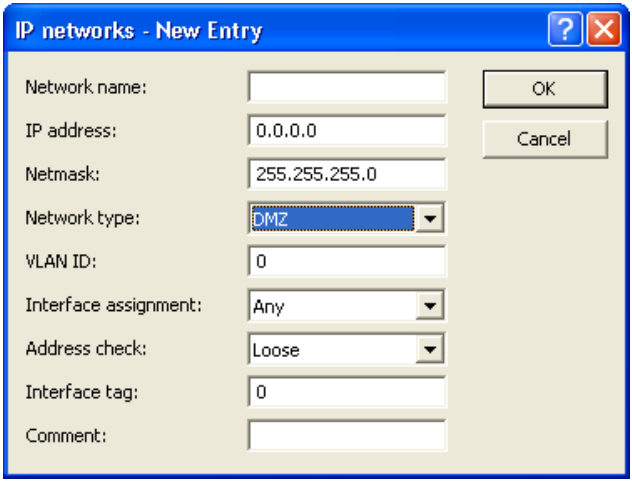
☐ Navigate to the following dialog:`Configuration : IPv4 : General` dialog and click "IP networks".



The DMZ network can be selected and edited from the "IP networks" window.

New additional networks can be added and assigned to the DMZ. To do so:

☐ In the ‘IP networks’ window, click ‘Add...’ to open the ‘New Entry‘ dialog:



☐ In this dialog, set the ‘Network type’ parameter to ‘DMZ’.

10.6.2 Address Checking

To shield the DMZ (demilitarized zone) and the Intranet from unauthorized attacks, you can activate an additional address check for each interface using the firewall's Intrusion Detection System, or IDS (see on page 736).

To configure address checking, do the following:

☐ In the "IP Networks - New Entry" dialog, select a setting for the "Address Check" parameter. Possible values:

- Loose: The OpenBAT device accepts any source address if the OpenBAT is directly addressed.
- Strict: The OpenBAT device requires that a return route has to be explicitly available so that no IDS notification is triggered. This is usually the case if the data packet contains a sender address to which the relevant interface can also route data. Sender addresses from other networks, to which the interface cannot route, or sender addresses from the local address range will therefore trigger an IDS-notification.

10.6.3 Unmasked Internet Access for a Server in the DMZ

While the inverse masquerading allows the (see on page 582) OpenBAT device to expose at least one service of each type (e.g. one Web, Mail and ftp server), this approach includes some restrictions:

- The masquerading module should support and "understand" the particular server service of the "exposed host." For instance, several VoIP servers use proprietary, non-standard ports for extended signaling. Such a server could be used exclusively on unmasked connections.
- Keep in mind that the "exposed host" resides within the LAN. When the host is under control of an attacker, it could be misused as a starting point for further attacks against machines in the local network.

Two Local Networks Operating Servers in a DMZ

This feature requires an Internet access with multiple static IP addresses.

Note: Please contact your ISP for an appropriate offer.

One example: For example: your ISP assigns you the IP network address 123.45.67.0 with the netmask 255.255.255.248. In this case, you can assign the following IP addresses:

DMZ IP address	Description
123.45.67.0	Network address
123.45.67.1	The OpenBAT device as a gateway for the Intranet
123.45.67.2	Device in the LAN which is to receive unmasked access to the Internet, e.g. web server connected at the DMZ port
123.45.67.7	Broadcast address

Computers and devices in the Intranet have no public IP address, and therefore appear with the IP address of the OpenBAT device (123.45.67.1) on the Internet.

Separation of Intranet and DMZ

Although Intranet and DMZ may already be separated at the Ethernet level by distinct interfaces, an appropriate firewall rule needs to be set up in all cases. In this way, the DMZ is also separated from the LAN at the IP level.

In this way, server service is available from both the Internet and the Intranet. However, IP traffic from the DMZ to the Intranet is not permitted. Extending the previous example:

- With an 'Allow All' strategy (default): Deny access from 123.45.67.2 to 'All stations in local network'.
- With a 'Deny All' strategy (see on page 699): Allow access from 'All stations in local network' to 123.45.67.2.

10.7 N:N Mapping

Network Address Translation (NAT) can be used to achieve several different goals:

- N:1 mapping:
  In N:1 NAT (also known as IP masquerading (see on page 579)), all addresses (‘N’) of the local network are mapped to just one (‘1’) public address. This clear assignment of data streams to the respective internal PCs is generally made available by the ports of the TCP and UDP protocols. For this reason, N:1 mapping is sometimes referred to as NAT/PAT (Network Address Translation/Port Address Translation).

  Due to the dynamic assignment of ports, N:1 masquerading enables exclusively those connections that have been initiated by the internal network. Exception: ‘inverse masquerading’ (see on page 582) where an internal IP address is statically exposed on a certain port.
- Network coupling:
  N:N mapping is used to couple networks with identical address ranges. This transforms unambiguously multiple addresses (“N”) of the local network to multiple (“N”) addresses of another network. This helps resolve address conflicts. Rules for address translation are defined in a static table in the OpenBAT device. Thereby new addresses are assigned to single stations, parts of the network, or the entire LAN, by means of which the stations can contact other networks.
- Remote monitoring and control:
  Some protocols (ftp, H.323) exchange parameters during their protocol negotiation, which can influence the address translation for the N:N mapping. For a correct functioning of the address translation, the connection information of these protocols is tracked appropriately by functions of the firewall in a dynamic table, and is additionally considered to the entries of the static table.

Note: The address translation is made ‘outbound’, i.e. the source address is translated for outgoing data packets and the destination address for incoming data packets, as long as the addresses are located within the defined translation range. An ‘inbound’ address mapping, whereby the source address is translated (instead of the destination address), needs to be realized by an appropriate ‘outbound’ address translation on the remote side.

10.7.1 Application Examples

The following examples of network coupling, and remote monitoring and control represent typical applications of N:N mapping.

Network Coupling

It is often desirable to couple the networks of two different companies that internally use the same private address range (e.g. 10.0.0.x). This occurs when one company needs to gain access to one (or more) servers of the other.

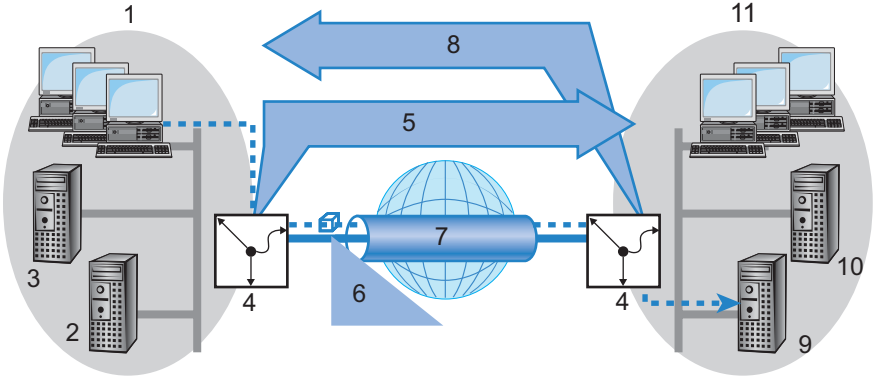


Figure 116:Network coupling

1: Network of company A	7: VPN tunnel
2: Server_A1: 10.0.0.1	8: N:N mapping to 192.168.2.x
3: Server_A2: 10.0.0.2	9: Server_B1: 10.0.0.1
4: Gateway	10: Server_B2: 10.0.0.2
5: N:N mapping to 192.168.1.x	11: Network of company B
6: Data packet - target: 192.168.2.1	–

In this example, network servers of company A and B need to gain access via a VPN tunnel to the other company's network. All stations of each LAN require access to the servers of the remote network. Initially, access to the other network is not possible, because each network uses the same address range. If a workstation on the company A network attempts to access server 1 of company B, the request (with an address from the 10.0.0.x network) will be routed exclusively within company A's local network; the inquiry will not even reach the gateway.

With the help of N:N mapping, all addresses of each LAN can be translated to a new address range for coupling with the other network. The network of company A is translated to 192.168.1.x. The network of company B is translated to 192.168.2.x. Using these new addresses, each LAN can now be reached from the other network. The station from the network of company A is now addressing server 1 of company B under the address 192.168.2.1. The addressee no longer resides within the network of company A. The inquiry is now passed on to the gateway, and is routed to the other network.

Remote Monitoring and Remote Control of Networks

Remote maintenance and control of networks is easier to accomplish by means of VPN. Using the nearly ubiquitous broadband Internet connections, a network administrator is not captive to multiple data communication technologies or expensive leased lines.

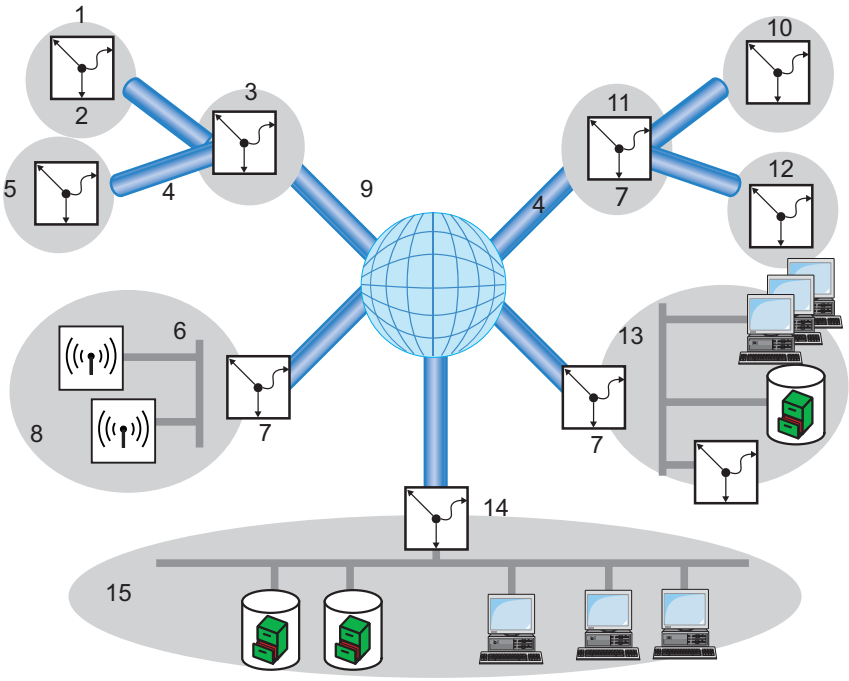


Figure 117:Centralized monitoring and control of networks for different clients

1: Customer A, office 1: 10.1.2.x, 255.255.255.0	9: Internet
2: Gateway, e.g. 10.1.2.1	10: Customer B, office 1: 10.1.2.x
3: Customer A, headquarters: 10.1.x.x, 255.255.0.0	11: Customer B, headquarters: 10.1.x.x, 255.255.0.0
4: VPN tunnel	12: Customer B, office 2: 10.1.3.x, 255.255.255.0
5: Customer A, office 2: 10.1.3.x, 255.255.255.	13: Customer D: 172.16.10.x, 255.255.255.0
6: WLAN, e.g. 172.16.10.11	14: Gateway, e.g. 80.123.123.123 (public) and 172.16.10.11 (intern)
7: Gateway	
8: Customer C: 172.16.10.x, 255.255.255.0	15: Service provider: 172.16.10.x, 255.255.255.0

In this example, a service provider monitors the networks of different clients out of a central control location. For this purpose, SNMP-capable devices should automatically send the respective trap notices of important events to the SNMP trap addressee (e.g. LANmonitor) of the network of the service provider. In this way, the LAN administrator of the service provider can dynamically view the current of the state of the devices at any time.

The individual networks can be structured very differently:

- Clients A and B integrate their branches with their own networks via VPN connections to each company LAN.
- Client C operates a network with several public WLAN base stations as hot spots.
- Client D includes an additional router for dial-up accesses in his LAN.

Note: The networks of client A and B use different address ranges in the respective head office and the connected branches. A standard network coupling via VPN is therefore possible between these networks.

In order to avoid the effort of creating its own VPN tunnel to each individual subnetwork clients A and B, the service provider makes just one VPN connection to the head office, and uses the existing VPN lines between head office and branches for communication with the branches.

Traps from the networks report to the service provider whether, e.g., a VPN tunnel is backed-up or lost, if a user has tried to log in three times with an incorrect password, if a user has attempted to establish a wireless connection, or if a LAN cable has been detached from a switch.

Routing of these different networks quickly reaches their address limits, if two or more clients use same address ranges. Additionally, if some clients use the same address range as the service provider, additional address conflicts are added. In this example, one of the hot spots of client C has the same address as the gateway of the service provider.

Here are two different approaches to resolve these address conflicts:

- Loopback decentralized 1:1 mapping:
  in the decentralized version, alternative IP addresses for communicating with the SNMP addressee are assigned to each of the monitored devices by means of 1:1 mapping. This address is in also known as a loopback address, and the method as the loopback method.

  Note: Loopback addresses are valid exclusively for communication with certain remote stations on the connections belonging to them. A OpenBAT device is thus not generally reachable at this IP address.

- Central N:N mapping:
  Instead of separately configuring each individual gateway in the branch networks, a better solution is for the administrator to configure a single central address translation in the gateway of the head office. At the same time, all subnetworks located behind the head office are also assigned the required new IP addresses.

In this example, the administrator of the service provider selects 10.2.x.x as central address translation for the network of client B, so that both networks configured with the same address range look like two different networks to the gateway of the service provider.

The administrator selects the address ranges 192.168.2.x and 192.168.3.x for client C and D, so that the addresses of these networks differ from the network of the service provider.

In order to enable the gateway of the provider to monitor the networks of clients C and D, the administrator also configures an address translation to 192.168.1.x for its own network.

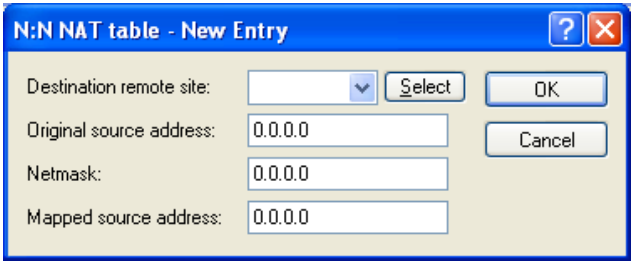
10.7.2 Configuring Address Translation

Configuration of N:N mapping requires very little information. Because a LAN can be coupled with several other networks via N:N mapping, different destinations can also have different address translations for a source IP range. The NAT table can contain a maximum of 64 entries.

To enter an item into the N:N NAT table:

☐ Navigate to the following dialog:`Configuration : IP-Router : N:N-Mapping` and click "N:N NAT table".

☐ Click "Add" to open the following dialog:



In this dialog, enter values for the following fields:

- Destination remote site:
  The name of the remote station to which this mapping rule will apply.
- Original source address:
  The IP address of the network to be mapped to a different address range for the specified remote station. This can be the address of a single station or of the router itself.
- Netmask:
  The netmask associated with the specified IP addresses. The netmask applies to both IP address ranges (original and mapped) because, for N:N address mapping, the original and the mapped IP networks need to be the same size. If you want to map just a single IP address, enter 255.255.255.255 for the netmask.
- Mapped source address:
  The IP address of the network to which the original addresses should be mapped for the specified remote station. The size of the mapped IP network depends on the specified netmask and is identical for the original and the mapped IP range.

When entering original and mapped source addresses, note the following:

- Original and mapped address can be assigned arbitrarily for the translation of single addresses. For example, it is possible to assign the mapping address 192.168.1.88 to a LAN server with the IP address 10.1.1.99.
- For translation of entire address ranges, the station-related part of the IP address will be taken directly, appended to the network-related part of the mapping address. Therefore, in an assignment of 10.0.0.0/255.255.255.0 to **192.168.1**.0, a server of the LAN with IP address 10.1.1.99 will get assigned the mapping address 192.168.**1.99**.

Note: The mapped address range should be at least as large as the source address range.

Note: N:N mapping functions are effective provided that the firewall has been activated.

Advanced Configuration Considerations

By setting up address translation in the NAT table, the networks and workstations become initially visible exclusively under the mapped address to devices in other networks. For seamless routing of data between networks, some further settings are still necessary:

- Entries in the routing tables for the new addresses so packets can find the way to their destination.
- DNS forwarding entries, in order that inquiries about certain devices in the other network can be resolved into mapped IP addresses (see on page 871).
- The firewall rules of the gateways need to be adjusted so that authorized stations in external networks can set up connections.

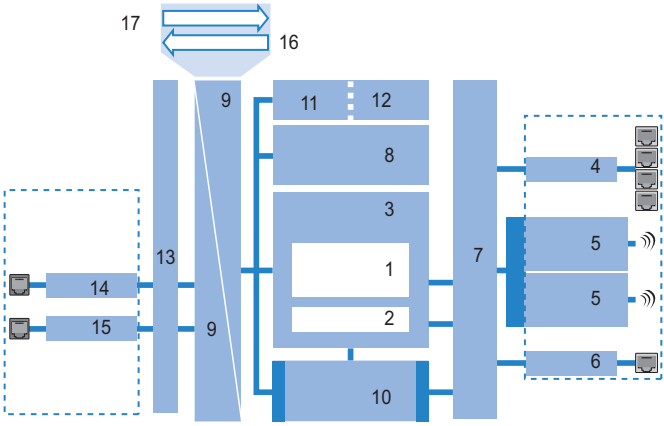


Figure 118:Address translation

1: IP router	10: Configuration & management
2: IP redirect	11: OpenBAT User administration
3: Firewall	12: RADIUS client / server
4: LAN interface or an integrated switch	13: DHCP client / PPP
5: Wireless modules	14: ADS
6: DMZ	15: DSL
7: LAN bridge	16: Source address
8: IP modules (NetBIOS, DNS, DHCP server, RADIUS, RIP, NTP, SNMP, SYSLOG, SMTP)	17: Destination address
9: IP masquerading and N:N mapping	

10.8 Establishing Connection with PPP

This routers also supports the point-to-point protocol (PPP). PPP is a generic term for a whole series of WAN protocols, which enable the interaction of routers made by different manufacturers. Because of the increasing importance of this family of protocols, and the fact that PPP is not associated with any specific routing operating mode, the following sections separately describe the device functions that are associated with PPP.

10.8.1 The Point-to-Point Protocol (PPP)

What is PPP?

The point-to-point protocol was developed specifically for network connections via serial channels and has become the standard for connections between routers. It implements the following functions:

- Password protection according to Password Authentication Protocol (PAP), Challenge Handshake Authentication Protocol (CHAP) or the Microsoft version of CHAP (MS CHAP)
- Callback functions
- Negotiation of the network protocol to be used over the established connection (IP or IPX, for example). Included in this are any parameters necessary for these protocols, for example IP addresses. This process is carried out using IPCP (IP Control Protocol).
- Negotiation of the connection parameters, e.g. the MTU (Maximum Transmission Unit (see on page 638).

- Verification of the connection through LCP (Link Control Protocol).
- Combining several DSL channels (MultiLink PPP, MultiLink PPPoE)

PPP is the standard used by router connections for communication between devices, or by the WAN connection software of different manufacturers. Connection parameters are negotiated and common settings are agreed using standardized control protocols (e.g., LCP, IPCP, CCP) that are contained in PPP.

PPP Application Scenarios

The point-to-point protocol is used in the following applications:

- for reasons of compatibility, for example, when communicating with external routers
- remote access from distant workstations
- Internet access (when sending addresses)

The PPP that is implemented by the OpenBAT device can be used synchronously or asynchronously, by either a transparent HDLC connection or an X.75 connection.

The Phases of PPP Negotiation

Establishing a connection using PPP begins with a negotiation of the parameters to be used for the connection. This negotiation is carried out in four phases which should be understood for the sake of configuration and troubleshooting:

- Establish phase:
  After a connection has been initiated at the data communication level, negotiation of the connection parameters begins through the LCP. This ascertains whether the remote site is also ready to use PPP. The packet sizes and the authentication protocol (PAP, CHAP, MS-CHAP or none) are determined. The LCP then switches to the opened state.
- Authenticate phase:
  Passwords are exchanged, if necessary. The password is sent just once if PAP is used for the authentication process. An encrypted password is sent periodically at adjustable intervals if CHAP or MS CHAP is used. A callback may also be negotiated in this phase via CBCP (Callback Control Protocol).
- Network phase:
  The OpenBAT device supports the protocols IPCP and IPXCP. After the password has been successfully transmitted, the IPCP and/or IPXCP network layer can be established. IP and/or IPS packets can be transferred from the router modules to the opened line if the negotiation of parameters is successful for at least one of the network layers.
- Terminate phase:
  In the final phase the line is cleared, when the logical connections for all protocols are cleared.

The PPP negotiation in the OpenBAT device

The progress of a PPP negotiation is logged in the devices' PPP statistics. The protocol packets listed in detail there can be used for checking purposes in the event of unusual system events. The PPP trace outputs offer a further method of analysis. You can use the command line interface command:

```
trace + ppp
```

to begin output of the PPP protocol frames exchanged during a terminal session. You can perform a detailed analysis once the connection has been broken if this terminal session has been logged in a log file.

10.8.2 Checking the Connection with LCP

The devices involved in the establishment of a connection through PPP negotiate a common behavior during data transfer. For example, they first decide whether a connection can be made using the specified security procedure, names and passwords.

The reliability of the connection can be constantly monitored using the link control protocol (LCP) after the connection has been established. This is achieved within the protocol by the LCP echo request and the associated LCP echo reply. The LCP echo request is a query in the form of a data packet which is transferred to the remote station along with the data. The connection is stable if a valid response to this request for information is returned (LCP echo reply). This request is repeated at defined intervals so that the connection can be continually monitored.

What happens if there is no reply? Initially, a few retries are initiated to exclude the possibility of any short-term line interference. The connection will be dropped and an alternative route sought if all the retries remain unanswered.

Note:

- During remote access of individual workstations with Windows operating systems, you may wish to switch off the regular LCP requests because these operating systems do not reply to LCP echo requests.
- The LCP request behavior is configured in the PPP list for each individual connection. Entries made in the ‘Time' and ‘Retries' fields set the intervals at which LCP requests should be made, and the number of retries that should be initiated without a response before the line can be considered lost. Setting both the ‘Time’ and the ‘Retries’ to ‘0’ turns off LCP requests (see on page 606).

10.8.3 Assignment of IP Addresses via PPP

In order to connect computers using TCP/IP as the network protocol, all participating computers require a valid and unique IP address. If a remote station does not have its own IP address (such as the individual workstation of a telecomputer), the OpenBAT device assigns it an IP address for the duration of the connection, enabling communications to take place.

This type of address assignment is carried out during PPP negotiation and implemented exclusively for connections via WAN. In contrast, the assignment of addresses via DHCP is (normally) used within a local network.

Note: Assignment of an IP address is possible provided that the OpenBAT device can identify the remote station by its call number or name when the call arrives, i.e. when the authentication process has been successful.

- Remote Access example:
  Address assignment is made possible by a special entry in the IP routing table. 255.255.255.255 is specified as the network mask, in addition to the IP address to be assigned to the remote site in the "Router-name" field. In this case, the router name is the name with which the remote site needs to identify itself to the OpenBAT device.

  In addition to the IP address, the addresses of the DNS and NBNS servers (Domain Name Server and NetBIOS Name Server) including the backup server from the entries in the TCP/IP module are transmitted to the remote station during this configuration.

  So that everything functions properly, the remote site also needs to be adjusted in such a way that it can obtain the IP address and the name server from the OpenBAT device. This can be accomplished with Windows dial-up networking through the settings in the "TCP settings" under "IP address" and "DNS configuration." This is where the options "IP address assigned by server" and "Specify name server addresses" are activated.
- Internet Access Example:
  If Internet access for a local network is accessed via the OpenBAT device, the assignment of IP addresses can occur in a reverse manner. In this case, configurations are possible in which the OpenBAT device itself has no valid IP address in the Internet and can be assigned one by the Internet provider for the duration of the connection. In addition to the IP address, the OpenBAT device also receives information about the DNS server from the provider during the PPP negotiation. In the local network, the OpenBAT device is known exclusively by its internal valid intranet address. Workstations in the local network can then access the same Internet account and also reach e.g. the DNS server.

Windows users are able to view the assigned addresses via LANmonitor. In addition to the name of the remote station, the current IP address as well as the addresses of DNS and NBNS servers can be found there. Options such as channel bundling or the duration of the connection are also displayed.

10.8.4 Configuring PPP Negotiation Settings

Use the PPP list to specify your own definition of PPP negotiation for each remote site contacting your network.

The authentication of point-to-point connections in the WAN commonly relies on one of the protocols PAP, CHAP, MS-CHAP or MS-CHAPv2. There exists a hierarchy among these protocols: MS-CHAPv2 is a "higher-level" protocol than MS-CHAP, CHAP or PAP. Higher-level protocols provide greater security. Many dial-in routers at Internet providers allow up-front authentication using a higher-level protocol such as CHAP, but support the use of PAP further down the line. If the setting for the protocol for authentication is fixed in the OpenBAT device, the connection may be lost because no common authentication protocol can be negotiated.

Note: In principle, authentication can be repeated during connection negotiation. Another protocol can be selected if, for example, it can be initially recognized from the username. However, this repeat negotiation is not supported in all scenarios. In particular when dialing in over UMTS, the OpenBAT device needs to explicitly refuse the provider's request for CHAP in order to be able to provide PAP user data for requests to be forwarded by the provider.

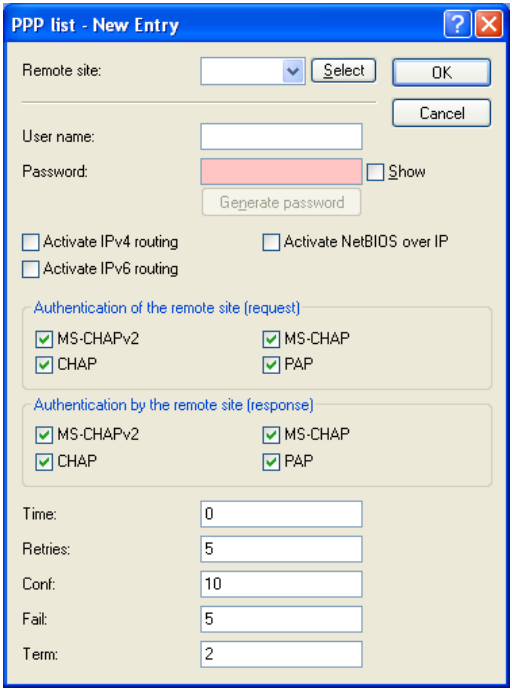
A flexible setting for the authentication protocols in the OpenBAT device establishes the PPP connection as required. In addition, one or more protocols can be defined that are accepted for authentication of remote sites in the OpenBAT device (inbound connections) and on login of the OpenBAT device into other remote sites (outbound connections).

- When establishing inbound connections, the OpenBAT device requires the lowest of the permitted protocols, but where possible it also permits the remote site to use one of the higher-level protocols.
- When establishing outbound connections, the OpenBAT device offers all enabled protocols, but permits just those that are selected. It is not possible to negotiate one of the disabled, possibly higher-level, protocols.

To access the PPP List, follow these steps:

☐ Open the `Configuration : Communication : Protocols` window, and click 'PPP list...'.

☐ In the 'PPP list', click 'Add...' to open the 'New Entry' dialog:



PPP negotiation is configured using the following parameters:

- Remote site:
  The name of the remote station, which needs to correspond to an entry in the list of remote sites (see on page 574).
- User name:
  The name under which the router should log in to the remote station. The router will use its own name if you leave this field blank.
- Password:
  The PPP password for the remote station. If your router has to log in to the remote station (e.g. an Internet provider), enter the log-in password here. If the remote station has to call your router, enter the log-in password with which the remote station will authenticate itself.

- Activate IPv4/IPv6 routing / Activate NetBIOS over IP:
  Select the protocols that are to be routed to the remote site.
- Authentication of the remote site (request):
  Specify the security measures that apply to the remote site when a connection is established. At least one of the selected measures needs to be responded to by the remote site. This is required by the local dial-in, for example. If the remote site is an Internet provider, select none of them. If more than one method is selected, a fallback to the next protocol is performed until the remote site successfully responds.
- Authentication by the remote side (response):
  Specify the security measures which are allowed for the local station when performing an authentication response. If the remote site is an Internet provider, select all of them. If none of the methods are selected, no local authentication is accepted from the remote site.
- Time:
  This parameter establishes the intervals at which cyclical checks should be performed for the remote station. For Windows remote stations, set this parameter to ‘0’.
- Retries:
  The number of attempted repetitions.
- Conf. / Fail / Term:
  These parameters affect the way PPP works. Please refer to RFC 1661 for detailed information. Normally, you can accept the default settings.

10.8.5 The DEFAULT Remote Site

During the PPP negotiation, the remote station dialing in logs into the OpenBAT device with its name. The OpenBAT device can derive the permissible values for authentication from the PPP table based on the name. At the start of the negotiation, the remote site occasionally cannot be identified by call number (dial-in), IP address (PPTP dial-in) or MAC address (PPPoE dial-in). It is thus not possible to determine the permitted protocols

in this first step. In these cases, authentication is performed first with those protocols enabled for the remote site with name DEFAULT. If the remote site is authenticated successfully with these settings, the protocols permitted for the remote site can also be determined.

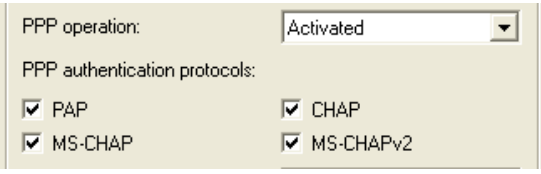
If authentication uses a protocol entered under DEFAULT, but which is not permitted for the remote site, then authentication is repeated with the permitted protocols.

10.8.6 RADIUS authentication of PPP connections

PPP connections can also be authenticated by an external RADIUS server. However, these external RADIUS servers do not necessarily support all available protocols. For this reason, the permitted protocols can also be selected in the configuration of the RADIUS authentication. LCP negotiation is restarted with the permitted protocols if the RADIUS server does not support the negotiated protocol.

To access the PPP List, follow these steps:

☐ Open the `Configuration : Communication : RADIUS` dialog. The PPP parameters are located in the middle of the dialog:



Configure the following parameters:

- PPP operation:
  Enable PPP authentication by the RADIUS server. In order to accomplish this, switch the PP. Select either:
  – Exclusive: the internal user authentication is ignored and the configured RADIUS server performs authentication.
  – Activated: the internal user authentication is the default authentication method.
- PPP authentication protocols:
  Specify the security measures which apply when authenticating a remote station. If the remote station is an Internet provider, which needs to be called by the router, de-select all choices. If all are selected, the next method will be used for authentication, if the previous did not achieve authentication. If none are selected, no authentication is required from the remote station.

10.9 PPPoE Servers

10.9.1 Introduction

As the availability of DSL has become widespread, point-to-point protocol over Ethernet (PPPoE) clients have been extensively integrated into device operating systems. PPPoE clients can be used to ‘log on to the network’ as well as to manage access rights to services such as the Internet, e-mail or remote stations.

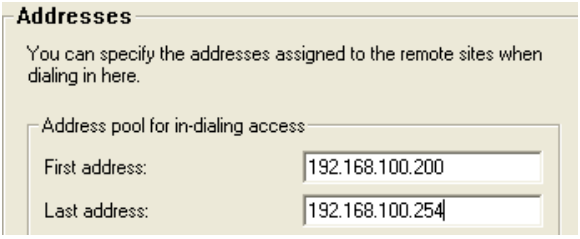
- **PPPoE: PPOE can only be used on one network segment**

  Because it is a layer 2 technology, PPPoE can be used exclusively within a network segment—i.e. it cannot be used across IP subnets. PPPoE connections cannot be established across network segment limits, such as via a router.

10.9.2 Example Application

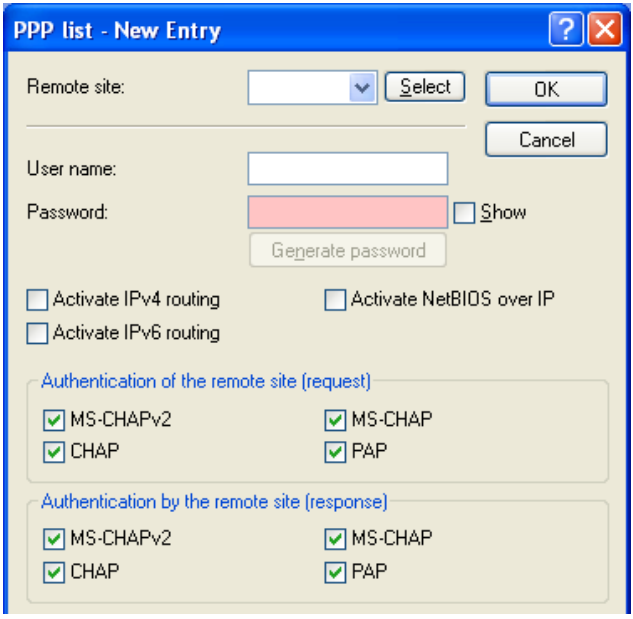
The following example illustrates the use of PPPoE:

- All employees in the Purchasing department need to first authenticate themselves to the OpenBAT device using PPoE (IP routing, PAP check) in order to access the Internet.
- All users in the LAN can directly access the OpenBAT device in its capacity as a router, firewall and gateway—i.e. there are no other routers between them. The computers in Purchasing are assigned an IP address from the address pool for dial-in addresses (192.168.100.200 - 192.168.100.254). This address range is configured in LANconfig in following dialog: `Configuration : TCP/IP :Addresses`.

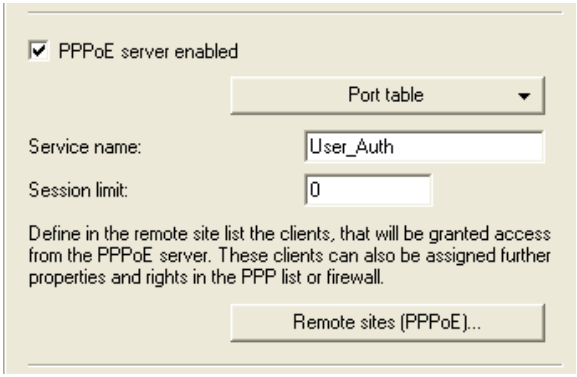


Note: The OpenBAT device itself is in a different IP Address range.

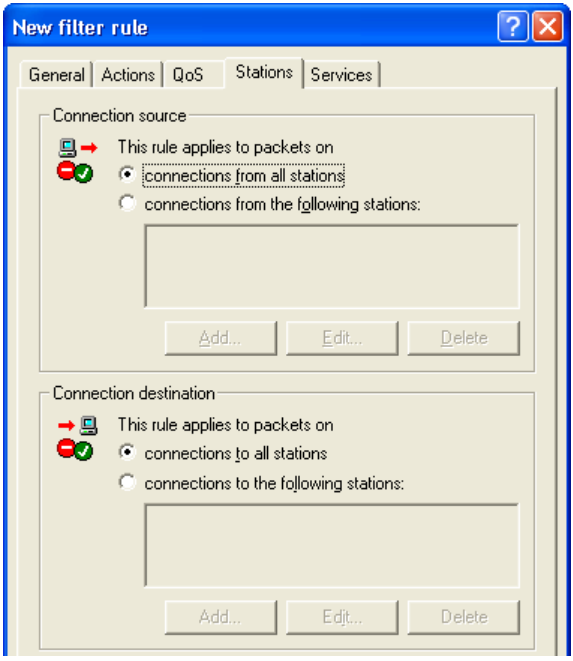
- To stop users from bypassing the authentication, a DENY ALL rule is defined in the firewall to stop local connections from being established.
- The user 'Purchasing' is then entered into the PPP list without a user name but with a password which is to be used by all staff members in the department, and authentication (encrypted) is set up as CHAP. Both IP routing and NetBIOS (Windows Networking) are to be activated for this PPP user. The "PPP list" can be accessed in LANconfig at: `Configuration : Communication : Protocols`.



- The PPPoe server is activated at: `Configuration : Communication : General` via the option "PPPoE server enabled".


PPPoE server enabled
Port table
Service name:
User_Auth
Session limit:
0
Define in the remote site list the clients, that will be granted access from the PPPoE server. These clients can also be assigned further properties and rights in the PPP list or firewall.
Remote sites (PPPoE)...

- Additional limitations (e.g. permissible MAC addresses) are also defined in the PPPoE server. This example uses the existing entry 'DEFAULT' with the MAC address '00.00.00.00.00.00', thereby permitting all MAC addresses. Refer to the section ‘Configuring PPPoE’ (see on page 615).
- Finally, firewall rules are created to control the services that are made available to the employees in Purchasing (e.g. release of http and e-mail exclusively). The firewall rules table can be accessed in LANconfig in the `Configuration : Firewall/QoS : Rules` dialog by clicking ‘Rules...’:

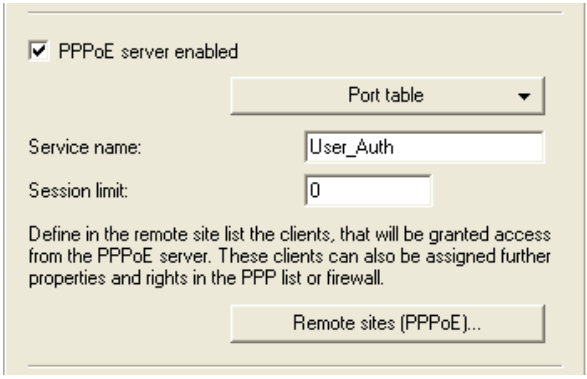


10.9.3 Configuring PPPoE

To configure PPPoE, follow these steps:

General PPPoE Settings

☐ Navigate to the following dialog:`Configuration : Communication : General`.


PPPoE server enabled
Port table
Service name:
User_Auth
Session limit:
0
Define in the remote site list the clients, that will be granted access from the PPPoE server. These clients can also be assigned further properties and rights in the PPP list or firewall.
Remote sites (PPPoE)...

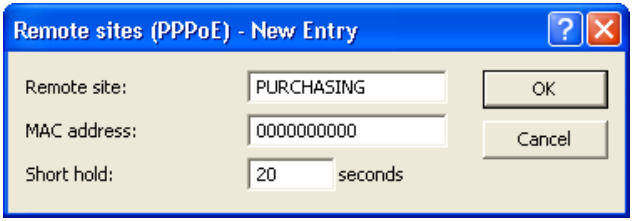
Enter settings for the following parameters:

- PPPoE server enabled:
  This selection enables and disables the PPPoE server.
- Service name:
  The name of the service offered. This enables a PPPoE client to select a certain PPPoE server that is entered for the client.
- Session limit:
  Indicate how often a client can be logged on simultaneously with the same MAC address. After the limit has been reached, the server stops responding to the client queries that are received. Default value is '1', maximum value '99'. A Session limit of '0' permits an unlimited number of sessions.

Adding Remote Sites (PPPoE)

☐ Navigate to the following dialog:`Configuration : Communication : General` and click "Remote sites (PPPoE)".

☐ In the ‘Remote sites (PPPoE)’ table, click ‘Add...’ to open the ‘New Entry’ dialog:



Enter settings for the following parameters:

- Remote site: The remote client’s PPP username.
- MAC address:
  If you specify a MAC address, the negotiation is terminated if the client logs on from a different MAC address. A MAC address of '000000000000' means that the client may log on with any MAC address.
- Short hold:
  The user's short hold time is set after the logon. If no entry exists, then the time belonging to user 'DEFAULT' is applied.

Note: In addition to this table, make an entry in the PPP table in which you enter the password, the rights (IP, IPX, NetBIOS) and other PPP parameters (LCP polling). The user can therefore also be authenticated using a RADIUS server. The "PPP list" can be accessed in LANconfig at: `Configuration : Communication : Protocols`.

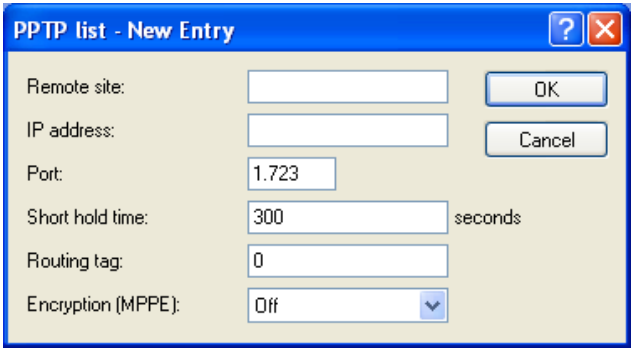
10.10DSL Dial-in over PPTP

Some DSL providers enable dial-in using the Point-to-Point Tunnelling Protocol (PPTP) instead of PPPoE. PPTP is an extension of PPP, partly developed by Microsoft. With PPTP it is possible to build up a ‘tunnel’ over IP networks to a remote station. A tunnel is a logical, shielded connection that secures the transferred data from unauthorized access, using the RC4 encoding algorithm.

The OpenBAT device can be configured for PPTP using the Setup Wizard, by selecting "Set up Internet access" and following the steps in that wizard. You can also manually configure PPTP, as follows:

☐ Navigate to the following dialog:`Configuration : Communication : Protocols` and click "PPTP list".

☐ In the "PPTP list", click "Add" to open the following dialog.



PPTP negotiation is configured using the following parameters:

- Remote site:
  The name of the remote station, which corresponds to an entry in the list of remote sites (see on page 574).
- IP address:
  The IP address of the PPTP gateway, often the address of the DSL modem.

- Port:
  The port the PPTP protocol runs on. For conformity with the protocol standard enter the port '1,723'.
- Short hold time:
  The time, in seconds, after which the connection should be closed if no data has been transferred. The value 9999 is used to establish an immediate connection of unlimited duration.
- Routing tag:
  This is used to evaluate the route of the respective PPTP server. This can be useful when running some PPTP ADSL modems, for example, those with the same IP address on different DSL ports.
- Encryption (MPPE):
  If you intend to secure the PPTP negotiation using the Microsoft Point-To-Point Encryption (MPPE) protocol (which also must be supported by the remote station), enter here the strength of the encryption.

10.11 Automatic Configuration of WLAN P2P Connections via Serial Interfaces

When P2P connections are configured in the WLAN area, the remote terminals usually recognize each other based on a specific characteristic of the respective P2P partner: either the station name or the MAC address of the P2P partner is entered in the configuration of the Access Points.
With changing P2P partners, you cannot permanently set this characteristic in the configuration. For example, if you want to establish a P2P connection between two train cars to offer IP services in the entire train, the respective P2P remote terminals change with every modification in the sequence of train cars.
In these cases, the Access Points can communicate the respective MAC addresses via the serial interface. For this purpose, you connect the devices via two wires of the serial interface (see Installation Guide). Then you set the identification of the P2P remote site to the value ‘serial autoconfig.’ Configure the P2P connections as with a fixed installation of Access Points.In default state, the WLAN modules are deactivated. When you switch on the devices, they communicate the MAC addresses, and only then do they activate the WLAN modules and automatically set up the P2P connection.

10.12 Keep Alive: Extended Connections for Flat Rates

Flat rates refer to connection fees that are not charged according to connection time but at a fixed price for fixed periods. Setting up a new connection is not worthwhile for flat rates

The keep-alive function of the OpenBAT device can be configured so that connections are re-established when the remote station has disconnected them.

The keep-alive function is activated by setting the "Short hold time" parameter for remote sites (peers) (see on page 574) Do one of the following:

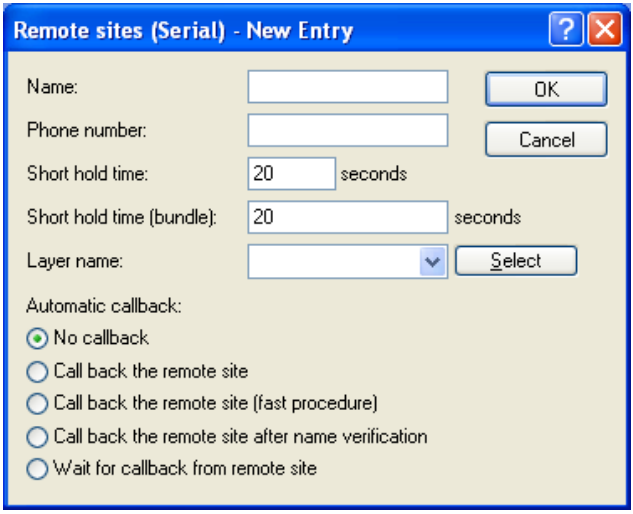
- 0 seconds: The OpenBAT device will not independently break the connection However, connections interrupted by the remote site are not automatically re-established if this value is used.
- 9999 seconds: The OpenBAT device automatically reestablishes the connection after every disconnection. In addition, the connection is reestablished after a reboot of the OpenBAT device.

10.13Callback Functions

Callback functions can be configured in LANconfig in the ‘Remote sites (Serial)’ dialog. To access this dialog:

☐ Navigate to the following dialog:`Configuration : Communication :Remote Sites` and click "Remote sites (Serial)".

☐ In the "Remote sites (Serial)" window, either add a new entry, or select and edit an existing entry:



10.13.1 Callback for Microsoft CBCP

For the Microsoft callback control protocol (CBCP), there can be various callback responses:

- the device called does not call back
- the device called allows the caller to specify the callback number
- the device called knows the callback numbers and calls these numbers exclusively

Via CBCP, it is possible to establish a connection to a OpenBAT device from a PC running the Windows operating system and to be called back by this PC. Three possible settings are selected in the remote sites list via the callback entry as well as the calling number entry.

- **No Callback**

  Automatic callback is set to ‘No callback’ (or set to ‘Off’ in WEBconfig or in the console).

- **Callback Number Specified by Caller**

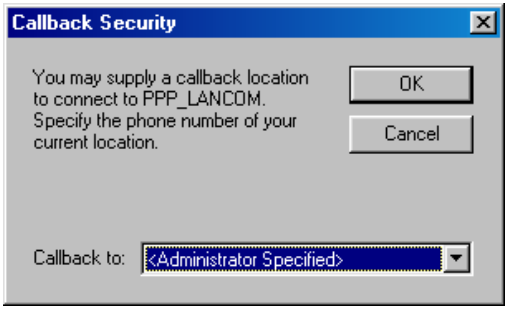
  - ☐ ‘Automatic callback’ is set to 'Call back the remote site after name verification', or needs to have the value 'Name' in WEBconfig or in the console.
  - ☐ No ‘Phone number’ setting may be specified.

  After the authentication, an input dialog appears on the caller's screen in Windows that requests the telephone number of the PC.

- **The OpenBAT device determines the callback number.**

  - ☐ "Automatic callback" must be set to "Call back the remote site after name verification" (or needs to have the value "Name" in WEBconfig or in the console).
  - ☐ One ‘Phone number’ value needs to be specified.

Some Windows versions (especially Windows 98) prompt the user to confirm the callback to the telephone number stored in the OpenBAT device ("Administrator Specified") with an input dialog. Other Windows versions inform the user that the PC is waiting for the callback from the OpenBAT device.



The callback to a Windows workstation occurs approximately 15 seconds after the first connection has been dropped. This time setting cannot be decreased since it is a Windows default setting.

10.13.2Fast Callback

Fast callback is ideal if two OpenBAT devices are to communicate with one another via callback.

In the device that is to be called back:

☐ Set "Automatic callback" to "Wait for callback from remote site" (or "Looser" when configuring via WEBconfig, terminal program or Telnet).

In the remote site (i.e., the callback party):

☐ Set "Automatic callback" to "Call back the remote site (fast procedure)" (or "fast" when configuring via WEBconfig, terminal program or Telnet).

☐ Specify one "Phone number" value.

Note: For fast callback using this method, keep up to date the number list for answering calls at both ends.

10.13.3 Callback via RFC 1570 (PPP LCP Extensions)

Callback via 1570 is the standard method for calling back routers from other manufacturers. This protocol extension describes five possibilities for requesting a call back. All versions are accepted by the OpenBAT device. The procedure is always the same: The OpenBAT device drops the connection after authenticating the remote station and then calls back the station a few seconds later.

To configure this version of callback, set "Automatic callback" to "Call back the remote site" (or select "Auto" in WEBconfig, the terminal program, or Telnet).

Note: For callback as per PPP, keep up to date the number list for answering calls in the OpenBAT device.

10.13.4 Overview of WEBconfig, Terminalprogram and Telnet

The following options are available in the peer list under WEBconfig and terminal program/telnet for the callback function:

Setting	Description
"Off"	No callback occurs.
"Auto"	The remote station will be called back if so specified in the peer list. Initially, the call is denied; as soon as the channel is clear again, the remote station is called back (duration is approximately 8 seconds). If the remote station is not found in the numerical list, it is first accepted as the DEFAULT remote station, and the callback is negotiated during the protocol negotiation. A charge of one unit is incurred.
"Name"	Before a callback occurs, a protocol negotiation is performed—even when the remote station was found in the numerical list (e.g. for computers with Windows having direct dialing on the device). Here minor charges result.
"fast"	When the remote station is found in the numerical list, a quick callback is carried out, i.e., the OpenBAT device sends a special signal to the remote station and calls back immediately when the channel is clear again. After approximately 2 seconds, the connection is established. If the remote station does not take back the call immediately after the signal, then after 2 seconds the situation reverts back to normal callback procedures (duration is once again approximately 8 seconds). This process is exclusively available for DSS1 connections.
Looser	Use this option when a callback is expected from the remote station. This setting carries out two functions simultaneously. First, it takes back a custom connection setup when there is an incoming call from the called remote station. Second, the function is activated with this setting to be able to react to the rapid callback procedure. Thus, in order to be able to use rapid callback, the caller needs to be in the "Looser" mode while the party being called needs to discontinue callback with "fast".

Note:

- The setting "Name" offers heightened security when an entry is made into the number list as well as the PPP list. The setting "fast" discovers the fastest callback method between two Hirschmann routers.
- With Windows remote stations, the "Name" setting needs to be selected.

10.14Operating a modem over the serial interface

Internationally, analog telephone connections are common in the business world. The operation of international networks places particular demands on remote maintenance options and for high-availability of the gateways. Apart from conventional analog telephone lines, mobile telephone networks such as GSM or GPRS may, in certain cases, represent the single way of providing remote maintenance without broadband or other cabled access.

In response to these requirements, OpenBATs with a serial interface can present an additional WAN interface, that is accessible via analog modems, GSM or GPRS. The following functions are available with a suitable modem in combination with a modem adapter:

- Internet access via modem with all of the router functions such as firewall, automatic connection establishment and termination, etc.
- Remote maintenance (e.g. dial-in to international sites)
- Backup connection (e.g. high-availability through GSM/GPRS modem connection)

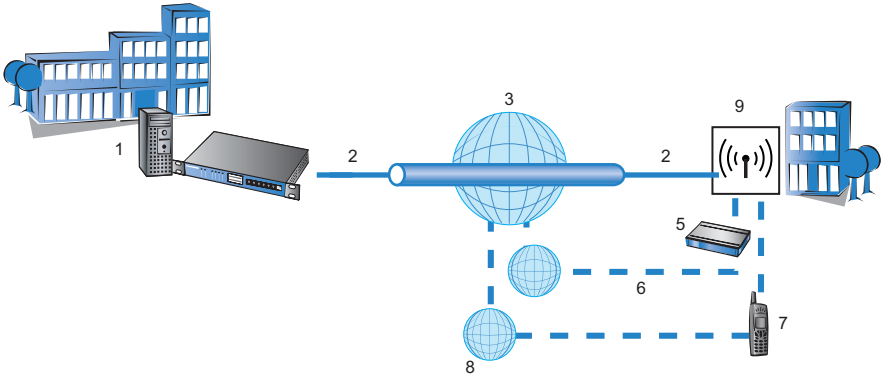


Figure 119:Operating a modem over the serial interface

1: Headquarters	6: Analog phone line
2: DSL	7: Modem (Global System for Mobile Communications (GSM)/General Packet Radio Service (GPRS))

3: Internet provider	8: GSM/GPRS
4: Secure connection	9: OpenBAT Device
5: Modem (analog)	–

10.14.1System Requirements

The following are required to set up a backup connection over the serial interface:

- A OpenBAT device with serial configuration interface and support for the modem adapter kit.
- LANconfig software (alternatively a web browser or CLI program)
- Serial configuration cable (supplied with the device)
- Analog modem, Hayes compatible, with access to a suitable analog telephone connection (D-sub9 or D-sub25 connector)
- Modem adapter to connect the modem over the serial configuration cable

10.14.2Installation

Perform the installation by connecting the modem to the serial configuration interface of the OpenBAT device, using a modem adapter.

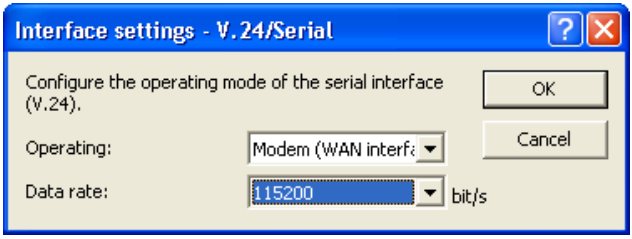
Note: Familiarize yourself with the contact assignments of the OpenBAT device (see on page 637).

10.14.3 Configuring the serial interface for modem operation

The operation of the serial interface requires the operating mode and bit rate to be set. To access these serial interface parameters:

☐ Navigate to the following dialog: `Configuration : Interfaces : WAN`.

☐ Click "Interface settings" and select "V.24/Serial".



In the 'Interface settings -V2.4/Serial' dialog, configure the following settings:

- Operating mode:
  Select one of the following settings:
  – Outband: the serial interface is used exclusively for configuration with a terminal program.
  – Modem: the device attempts to find a modem connected to the serial interface. If this is successful then the modem can be used as an additional WAN interface. If a computer running a terminal program is detected, then the device automatically switches the interface to outband mode.
- Data rate:
  the maximum bitrate supported by the modem. The serial interfaces of OpenBAT devices support data rates of 19,200 bps, 38,400 bps, 57,600 bps up to a maximum of 115,200 bps.

Note: While a OpenBAT device is set to "Modem" operating mode, a terminal program operating over the serial interface will display the AT commands that the OpenBAT device transmits while attempting to identify a connected modem. In the terminal program, press the return key repeatedly until the modem identification is interrupted, and start the configuration session.

10.14.4 Configuring Modem Parameters

The operation of a modem at the serial interface is configured using the following WAN and Modem interface settings.

☐ Navigate to the following dialog: `Configuration : Interfaces : WAN`, to configure the following parameters:

- Request modem ID (default = 16)
- Reset command (default = &F)
- Initialize command (default = L0X1M1S0=0)
  - L0: Loudspeaker quiet
  - X1: Operation at an extension
  - M1: Loudspeaker on while connecting
  S0=0: Disable auto answering
- Deactivate modem echo (default = E0)

☐ Navigate to the following dialog: `Configuration : Interfaces : Modem`, to configure the following parameters:

- AT polling cycle time (default = 1 second)
- AT polling count (default = 5)
- Ring count (default = 1)
- Initialize answer command
- Answer command (default = A)
- Initialize dial command
- Dial command (default = DT)
- Escape sequence—to terminate data phase response to return to command phase (default = +++)
- Wait after escape sequence (default = 1000 ms)
- Disconnect command (Default = H)

Note: The modem parameters are set with values that should suit most modems. Changes are usually not necessary. Refer to the documentation for your modem for settings that vary from these.

Configuring a GPRS Backup Connection

If the connection is to use a GPRS-capable modem at the serial interface, you will need the APN name and the dial-up telephone number. The following init-strings for the configuration apply to T-Mobile and Vodafone:

- T-Mobile:

Init-string:

```
L0X1M1S0=0+CGDCONT=1, "IP", "internet.t-d1.de"
```

Dial-up number:

```
*99#
```

- Vodaphone:

Init-string:

```
L0X1M1S0=0+CGDCONT=1, "IP", "web.vodafone.de"
```

Dial-up number:

`*99#` or `*99***1#`

Entering Special Characters in the Console

For a GPRS dial-up, the initialization strings require the entry of inverted commas and equal signs. Certain special characters can be correspondingly marked with a leading backslash:

- `*`
- `"`
- `=`
- space

Example:

```
+cgdcont\=1,\"IP\",\"internet.t-d1.de\"
```

As an alternative, the entire command sequence can be enclosed within inverted commas. In this case, those inverted commas which are inside the surrounding inverted commas needs to be preceded by a backslash:

Example:

```
”+cgdcont=1,\”IP\”,\”internet.t-d1.de\””
```

10.14.5 Direct Entry of AT Commands

The following command allows you to use Telnet to send a character string directly to a modem that is connected to the OpenBAT device:

```
sendserial "AT..."
```

This function allows you to send any AT commands to the modem.

Note: Sending AT commands is possible exclusively in the internal modem state "idle" or "Modem ready." The responses can be found in the serial trace.

10.14.6 Statistics

Statistics about activities of the serial interface can be accessed with a terminal program or Telnet under:

```
Status/Modem-Status
```

The statistics show the following states:

- the type of modem identified
- the status of its last connection, e.g. the transfer rate, the transfer protocol used or the exception-detection method used
- internal state of modem management, for example:
  - Discovery
  - interface deactivated
  - modem initialization
  - modem ready
  - Connection setup
  - modem in data mode

  These messages may be very helpful for debugging purposes.

10.14.7 Trace Output

The following command allows you to start the trace output for the serial interface in a Telnet session when a OpenBAT device has a modem connected:

```
trace + serial
```

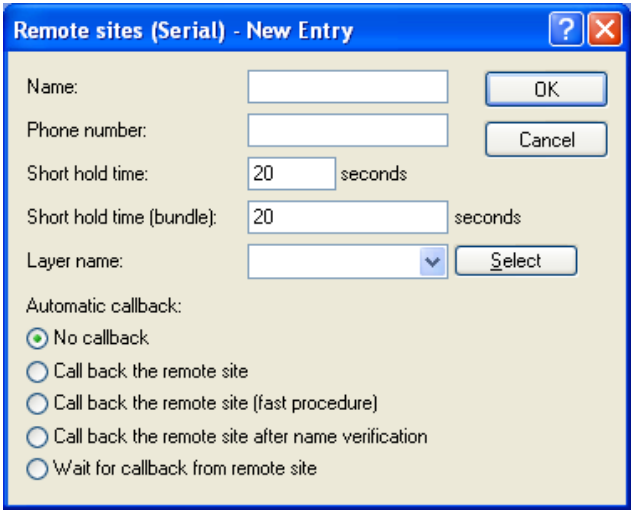
The output shows all messages exchanged up until the establishment of data transfer between the modem and the OpenBAT device.

10.14.8 Configuring Remote Sites for V.24 WAN Interfaces

To establish a connection to a remote station via the modem connected to the serial interface, create a corresponding entry in the remote sites (serial) list (see on page 574). To create a remote site list entry for a serial connection, follow these steps:

☐ Navigate to the following dialog:`Configuration : Communication :Remote Sites` and click "Remote sites (Serial)".

☐ In the 'Remote sites (Serial)' window, click 'Add...' to open the 'New Entry' dialog:



Configure the following settings for a serial connection:

- Name:
  Name of the remote site.
- Telephone number:
  The telephone number that reaches the remote site. The field can be left empty if calls are to be received exclusively.

- Short Hold time:
  This time defines how long a connection is kept active even if no more data is being transferred. If a zero is entered, the connection will not be interrupted automatically. A short hold time of ’9999’ means that the connection is held open indefinitely. If it is interrupted, then the connection will be actively opened up again. This behavior is known as keep alive.
- Short hold time (bundle): This is ignored
- Layer name:
  Select 'V.24_DEF' for the connection over the serial WAN interface. The layer is preset and does not need further configuration. The layer 'V.24_DEF' uses the following settings:
  – Encapsulation: Transparent
  – Layer 3: APPP (asynchronous PPP)
  – Layer 2: Transparent
  – Options: none

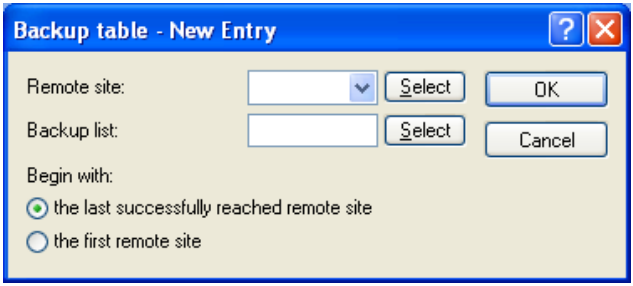
After an entry in the remote site (serial) list has been generated for the WAN interface, this remote station can be used just like any other for routing and WAN connections.

10.14.9 Configuring a Backup Connection on the Serial Interface

The configuration of a backup connection via a modem at the serial interface includes the following configuration entries:

☐ a dial-up peer station in the ‘Remote sites (Serial)’ table (see on page 574)

☐ a backup remote station entry in the "Backup table". Access this table at `Configuration : Communication : Call Management`.

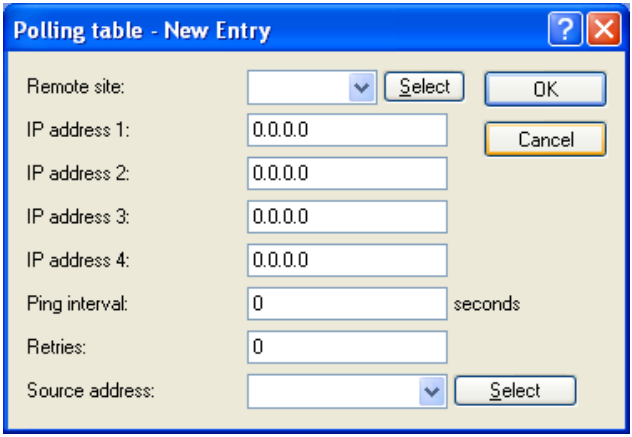


For each entry, configure the following parameters:

- Remote site:
  The remote site that is to be called by the modem at the serial interface.
- Backup list:
  The backup remote stations. Use exactly the same names that have been entered in the list of remote sites. Separate the individual remote stations with semicolons.
- Begin with:
  The order in which remote stations in the backup list are called.

☐ an entry in the ‘Polling table’ may be needed if the link to the remote station to be backed up cannot be checked by LCP polling (with PPP exclusively). This involves assigning the remote site with an IP address that can be regularly tested with a ping command. The IP address should typically be a computer directly at the opposite end of the connection being tested, e.g. a DNS server in your provider's network.

In the `Configuration : Communication : Remote Sites` dialog, click "Polling table".



For each entry, configure the following parameters:

- Remote site:
  The remote site that is to be called by the modem at the serial interface.
- IP address 1...4:
  A list of up to 4 IP addresses that will be pinged in sequence to check the connection state of the remote site. The connection is evaluated as intact as long as at least one specified IP address can be reached successfully. Select IP addresses that are continuously reachable. Otherwise, there will be needless and possibly costly backup connections.
- Ping interval:
  The interval, in seconds, between pings. If you set the ping interval and the number of retries to 0, defaults will be used to check the connection.

- Retries:
  The number of retries in case there is no response to a ping. Retries are sent once per second. The connection will be terminated if no response is received. If you set this value and the ping interval to 0, defaults will be used to check the connection.
- Source IP address:
  An optional source address that can be used instead of the source address, which is otherwise obtained automatically for the respective destination address. When loopback addresses are configured, they can be used as source address here.

10.14.10 Contact Assignment of Modem Connectors

Device signal	D-Sub9 plug	Device or modem signal	D-Sub9 plug
TxD	3	RxD	2
RxD	2	TxD	3
RTS	7	CTS	8
CTS	8	RTS	7
DTR	4	DCD	1
DCD	1	DTR	4
GND	5	GND	5

10.15 Manual Definition of the MTU

Many Internet providers operate their own backbone, but their customers dial in to the network over the access nodes of third-party telecommunications providers. This "two-stage" dial-in procedure can lead to problems with the resulting data rate:

- When dialing into the nodes of Deutsche Telekom, for example, a OpenBAT device negotiates a permissible maximum transmission unit (MTU), which defines the greatest possible size of unfragmented data packet. This MTU is then also used by the OpenBAT device.
- When the data packets are forwarded to the actual provider, an additional header is added that again increases the size of the data packets. For the data packets to meet maximum size limits, they need to be fragmented into smaller units. This additional fragmentation can cause reduction in data-transfer speeds.

This situation can be avoided by entering a fixed MTU for each remote site.

10.15.1 Configuring the MTU

Enter an MTU setting for remote sites using WEBconfig as follows:

☐ Navigate to the following dialog:

`Hirschmann Menu tree : Setup : WAN : MTU-List`

Configure the following parameters for each MTU entry:

- Remote site: the name of the device in the remote sites list.
- MTU: the maximum size, in bytes, of a data packet that can be transmitted over the connection to the remote site.

10.15.2 Statistics

To view MTU statistics in WEBconfig, navigate to the following location:

Hirschmann Menu tree : Status : WAN : MTU

The table is partially dynamic and begins with 16 entries. It includes two columns in which the device name and the MTU are stored.

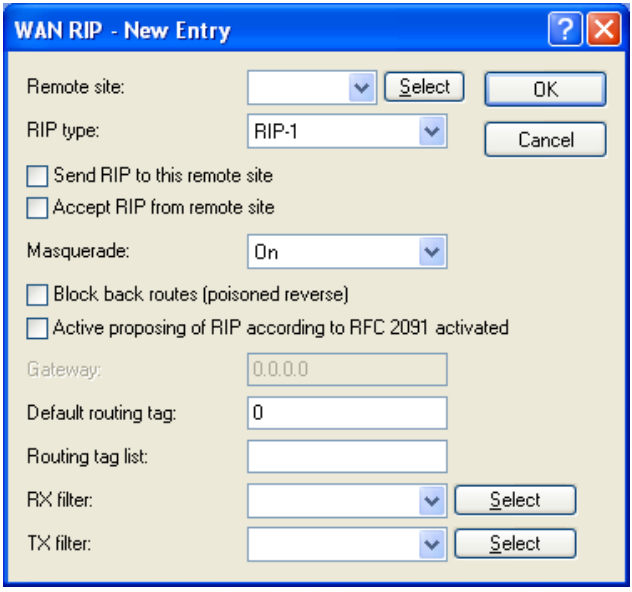
Note: MTU lists and MTU statistics are available exclusively for devices with a DSL or ADSL interface.

10.16WAN RIP

To enable routes learned from RIP to be broadcast across the WAN, enter the respective remote sites into the WAN RIP table. To make an entry into the WAN RIP table, follow these steps:

☐ Open the `Configuration : IP Router : General` dialog and click ‘WAN RIP...’.

☐ In the ‘WAN RIP’ table, click ‘Add...’ to open the ‘New Entry‘ dialog:



Configure the following settings for each entry:

- Remote site:
  The name of the remote site.
- RIP type:
  The version of RIP used to propagate local routes.
- Send RIP to this remote site:
  Select this to enable the sending of RIP route data to the selected remote site.

- Accept RIP from remote site:
  Select this to enable the receipt of RIP route data from the selected remote site.
- Masquerade:
  This indicates whether or not masquerading is enabled on the connection and how it is implemented. This entry makes it possible to start WAN RIP even with an empty routing table. Settings include:
  – Auto: The masquerade type is taken from the routing table (value: 0). If there is no routing entry for the remote site, then masquerading is not performed.
  – On: All connections are masqueraded (value: 1).
  – Intranet: IP masquerading is used for connections from the intranet, connections from the DMZ pass through transparently (value: 2)
- Block back routes (poisoned reverse):
  When you select this, routes learned/received via this interface are marked as 'not reachable' and sent back with the hop count directly set to 16, the maximum count (see on page 558).
- Active proposing of RIP according to RFC 2091 activated:
  For active connections (according to RFC 2091), there is a fallback to 'normal' RIP according to RFC 2453: the fallback is initiated if the remote site does not answer after 10 retries of the first packet (10 retries last approximately 30 seconds).
- Gateway:
  If ‘Active proposing of RIP...’ is selected, the IP address of the RIP partner on the remote side of the WAN connection has to be entered as gateway. It is possible to enter 0.0.0.0 here if a PPP negotiation is established on the WAN connection and thereby the IP address of the remote site is transferred.
- Default routing tag:
  The column Default tag lists the valid ’Default routing tag’ for the WAN connection. All untagged routes are tagged with this tag when sent on the WAN.

- Routing tag list:
  A comma-separated list of the tags that are accepted on the interface. If this list is empty, then all tags are accepted. If at least one tag is in the list, then just the tags in this list are accepted. When sending tagged routes on the WAN, exclusively routes with valid tags are propagated. All learned routes from the WAN are treated internally as untagged routes and propagated on the LAN with the default tag (0). In the WAN, they are propagated with the tag with which they were learned.
- Rx/Tx filter:
  Select the filters to be used on receiving (RX) and transmitting (TX) RIP packets. Items in this list are taken from the ‘RIP Filter’ list (see on page 554).

10.17 The Rapid Spanning Tree Protocol

In networks with numerous switches and bridges, multiple physical connections can exist between two stations that are connected to the network. These redundant data paths are desirable because they can offer alternative paths to the desired destination if one network path ceases to operate. However, multiple connections can also create loops or cause network stations to receive duplicate frames. Both of these events negatively impact network performance.

The spanning tree protocol (STP) enables an analysis of the network at the layer 2 level and offers solutions for intelligent path selection between two network stations below the routing layer. By discovering redundant paths between network stations, STP builds a unique structure in which loops and duplicate packets can be avoided. STP sends Bridge Protocol Data Units (BPDUs) as a multicast to a specific MAC address. The BPDUs let STP discover redundant paths, as well as the distance and the data rate available on each connection. Using these values, STP calculates a priority (also called route or path costs) for each connection. Low-priority connections are disabled and thereby made unavailable to clients. By disabling all but the non-redundant connections between clients, the protocol builds a tree which unambiguously defines all of the connections that arise from a central switch (root bridge).

BPDUs are regularly transmitted over the network to check the availability of the connections. If a connection ceases to function, network analysis is triggered again, and network paths and their priorities are redefined. After initialization, all ports are initially in the “blocking” state, in which just BPDUs are transmitted. The ports subsequently switch to the states of ’listening’ and then ’learning’ before reaching ’forwarding’ which allows payload data to be exchanged via the ports.

10.17.1 Classic and Rapid Spanning Tree

The early version of the spanning-tree protocol (compliant with IEEE 802.1D)—here referred to as classic spanning tree—implemented topology changes very slowly after a connection break was detected. Depending on the complexity of the network, classic spanning tree protocol requires from 20 seconds to a minute to establish new routes. For many network services, a delay of this duration is unacceptable.

The spanning tree protocol was improved and published as the "rapid spanning tree protocol" (RSTP), initially as the IEE 802.1t/w standard and later as a part of the newly published IEEE 802.1D. The OpenBAT device supports both the classic and rapid versions of STP.

10.17.2RSTP Improvements

The primary aim of RSTP is to accelerate the activation of network paths after an active connection is lost. RSTP achieves this by dispensing with the states 'blocking' and 'listening' to reduce the time required to update the network paths to just a few seconds. In case of a network path disconnection, not all of the links are blocked until the new topology has been calculated. Instead, just the lost connections are unavailable for use. RSTP also allows a network administrator to edit network topology settings.

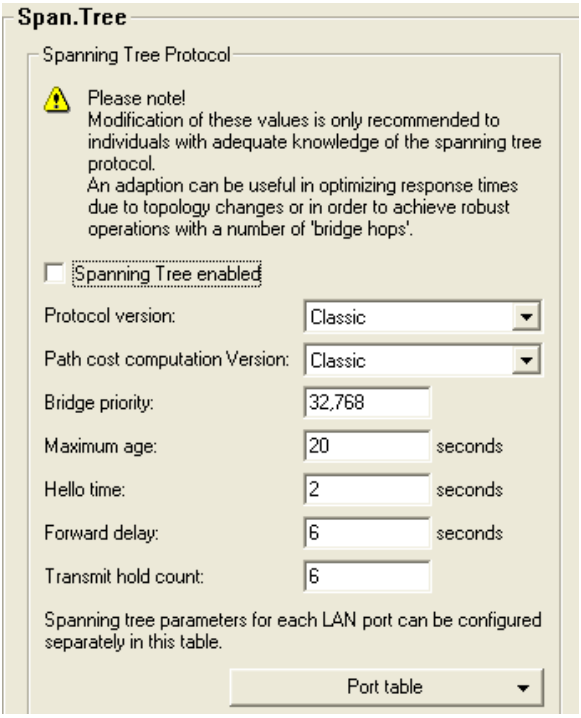
- A bridge port can be defined as an edge port. An edge port is the exclusive bridge port leading to the connected LAN segment. No additional bridges can be connected to the LAN segment, just workstations, servers, etc. Because these ports cannot lead to loops, they change immediately into the forwarding state without waiting for the network topology to be determined. However, RSTP continues to monitor these ports. If BPDUs are unexpectedly received at an edge port due to another bridge being connected to the LAN, the port automatically returns to its normal state.
- A bridge port can also operate as a point-to-point link. In this case the port is directly connected with an additional bridge. Since no additional stations can be positioned between the two bridges, the change into the forwarding state can take place faster.

In the ideal case, RSTP immediately resorts to familiar alternative network paths in case of connection loss.

10.17.3 Configuring the Spanning Tree Protocol

To configure parameters for RSTP or STP functionality, make edits to both the general RSTP parameters and the port table, as follows:

☐ Navigate to the following dialog: `Configuration :Interfaces : Span.Tree`.

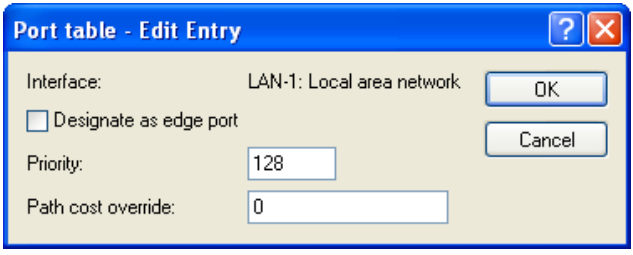


General STP settings:

- Spanning tree activated
  Toggles STP support on and off. When STP is turned off, a OpenBAT device does not send any spanning tree packets, and forwards received packets instead of processing them.
- Protocol version:
  Either the classic or RSTP version of the protocol.

- Path cost computation version:
  The version of spanning tree used to compute path costs, either the classic or RSTP version of the protocol.
- Bridge priority:
  The priority of the bridge in the LAN. This can influence which bridge should preferably be made root bridge by the protocol. To maintain compatibility with RSTP, this value should be adjusted in multiples of 4096, because RSTP uses the lower 12-bits of this 16-bit value for other purposes.
- Maximum age:
  This value defines the time (in seconds) after which a bridge drops messages received through Spanning Tree as "outdated." This parameter defines how quickly the Spanning Tree algorithm reacts to changes.
- Hello time:
  This parameter defines (in seconds) the intervals a device—selected to be the root bridge—sends Spanning Tree information into the LAN.
- Forwarding delay
  This time (in seconds) determines how much time needs to pass at a minimum before a Spanning Tree port can change the status (listening, learning, forwarding). When using RSTP the forwarding delay often has no effect, because RSTP has suitable mechanisms of its own to prompt a rapid switching into the forwarding state.
- Transmit hold count:
  The number of BPDUs which can be transmitted by RSTP before a one second pause commences. When using classical STP the transmit-hold count has no effect.

To make edits to Port table settings, click ‘Port table’ and select an available port (LAN, wireless LAN, point-to-point connections):



Configure the following parameters for each selected port:

- Designate as edge port:
  Marks the port as an edge port that is not connected to any other bridges, but exclusively to workstations or servers. Edge ports switch immediately into the forwarding state. Edge ports continue to be monitored by RSTP. If a port of this type receives BPDUs, then its status as an edge port is removed.
- Priority:
  The priority of the port. In the case of multiple network paths with identical path costs, the priority value decides which port is used. If priority values are identical, the port to be used is the first in the list. To maintain compatibility with RSTP, this value may be adjusted in steps of 16 because RSTP uses just the upper 4-bits of this 16-bit value.
- Path cost override:
  This setting controls the priority of paths with equal value. The value set here is used to make the selection instead of the computed path costs. A value of ‘0’ turns off this override.

10.17.4Status Reports for Spanning Tree

Current spanning tree values can be monitored via Telnet or WEBconfig. To view the status of spanning tree parameters, navigate to the following location in WEBconfig:

```
Hirschmann Menu tree : Status : LAN-Bridge-
Statistics : Spanning-Tree
```

General Status Information

The following spanning tree parameters are displayed:

- Bridge ID:
  The ID for the device that is being used by the spanning tree algorithm. It is composed of the user-defined priority (upper 16 bits) and the device MAC address (lower 48 bits).
- Bridge Priority:
  The priority of the LAN bridge within the root bridge detection process.
- Operating:
  Operating status of the port.
- Path Cost Computation:
  The protocol version currently set for computing path cost.
- Protocol Version:
  The protocol version currently set for determining network topology.
- Root Bridge:
  The ID for the device that is currently elected root bridge.
- Root Path Cost:
  The path costs of all hops added together in order to reach the root bridge from this device.
- Root Port:
  The port that can be used to reach the root bridge from this device. If the device itself is the root bridge, it is displayed with the special value '255'.

Port Table Information

The port table can be used to inspect the following values for all available ports (LAN, wireless LAN, point-to-point connections):

- Priority:
  The priority of this port taken from the port configuration.
- Status:
  The current status of the port:
  - disabled: no packets can be sent or received through this port. This occurs when the port has either been disabled manually or when it has a negative link status.
  - Listening: Intermediate state on the way to enabling. Only spanning tree packets are listened to, data packets are ignored and are also not forwarded to this port.
  - Learning: Further intermediate state. As opposed to "listening" additional MAC addresses from data packets entering this port are learned but data packets are still not forwarded.
  - Forwarding: Forwarding: the port is completely active, data packets are received and forwarded in both directions.
  - Blocking: Spanning tree has identified this port to be redundant and disabled it for data traffic.
- Root:
  The ID of the root bridge that can be reached through this port.
- Bridge:
  This is the ID of the bridge through which the root bridge can be reached.
- Path cost:
  The value is determined by the port technology (Ethernet, WLAN, etc.) and the bandwidth. Examples of values used are:

Transfer technology	Costs of Classic STP	Costs of RSTP
Ethernet 10 MBit	100	2000000
Ethernet 100 MBit	19	200000
Ethernet 1000 MBit	4	200000
WLAN 2 MBit	500	12500000
WLAN 11 MBit	140	4000000
WLAN 54 MBit	35	900000
WLAN 108 MBit	25	450000

Note: If path costs for a port were manually entered, then the configured value appears in this column.

RSTP Port Statistics Information

The RSTP port table can be used to inspect the following values for all available ports (LAN, wireless LAN, point-to-point connections):

- Role: Root or Non-root bridge.
- Learning: Port in learning state.
- Forwarding: Port in forwarding state.
- Edge Port: Port defined as an edge port.
- Protocol Version: Classic or Rapid.
- Costs: Setting for this port's cost

10.18The Action Table

The action table controls actions triggered when there is a change in the status of WAN connections. WAN connections include direct connections to an Internet provider. Every action is linked with a condition that describes the change in status of the WAN connection (establishment, termination, failure or establish failure). Actions include any of the commands available at the Telnet console. Furthermore, actions can transmit messages by e-mail or SYSLOG, send an http request, or transmit a DNS request. Variables allow information—for example, the current IP address, the name of the device, or an exception response—to be integrated into the action.

10.18.1Actions for Dynamic DNS

Systems with dynamic IP addresses can be made available for access via the WAN, for example via the Internet, by using the services of commercially available dynamic DNS servers. Servers offering these services can assign the current IP address of a device to its FQDN name (Fully Qualified Domain Name, e. g. “http://MyDevice.dynDNS.org”).

The advantage is obvious: If you wish to carry out remote maintenance via WEBconfig/http, for example, you need just the dynamic DNS name.

In order for the current IP address to match the DynDNS name at all times, the IP address recorded on the DynDNS server needs to be constantly updated. This change is triggered by a dynamic DNS client.

- The DynDNS server, maintained by a DynDNS service provider on the Internet, is in contact with the Internet DNS servers.
- The Dynamic DNS client can run on a workstation as a separate client program. Alternatively, a Dynamic DNS server is integrated into the OpenBAT device. It can make contact to any one of a number of dynamic-DNS service providers and, assuming that a user account has been set up, automatically update its current IP address for the DNS name translation.

Dynamic DNS Client on the Workstation

Dynamic DNS providers support a range of PC client programs that use various methods to determine the IP address currently assigned to a OpenBAT device. A change in IP address is communicated to the appropriate dynamic DNS server.

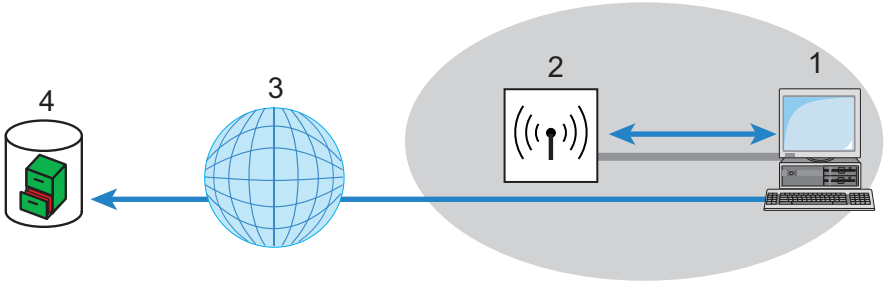
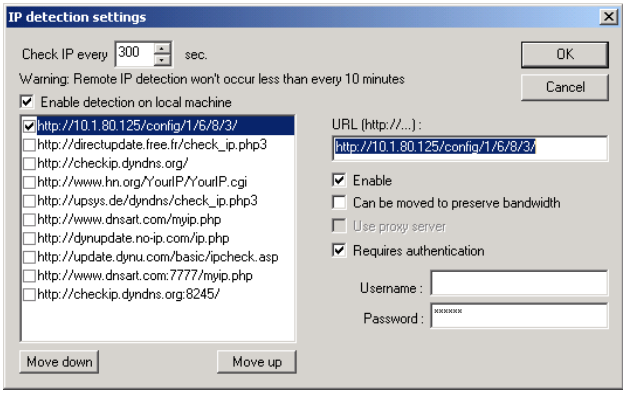


Figure 120:Dynamic DNS client on the workstation

1: PC with DynDNS client	3: Internet
2: OpenBAT Device	4: Server at DynDNS provider

The current WAN-side IP address of a device can be read from the following address and entered into a client program:

```
http://<Address of the Device>/config/1/6/8/3/
```



Note: The above screenshot illustrates how to access the WAN IP address on the WEB interface from an external application.

Dynamic DNS client in the OpenBATvia HTTP

Alternatively the OpenBAT device can directly transmit the present WAN IP to the DynDNS provider:

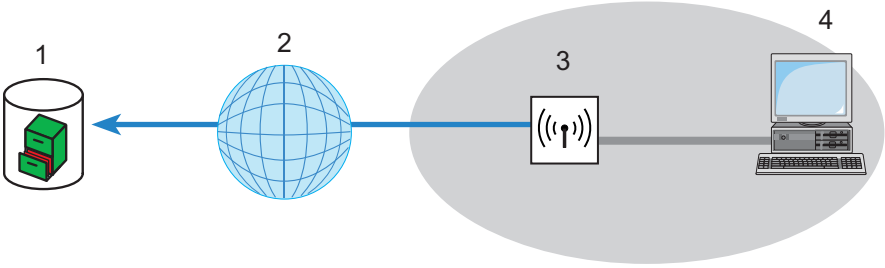


Figure 121:Transmitting the current WAN IP to the DynDNS provider directly

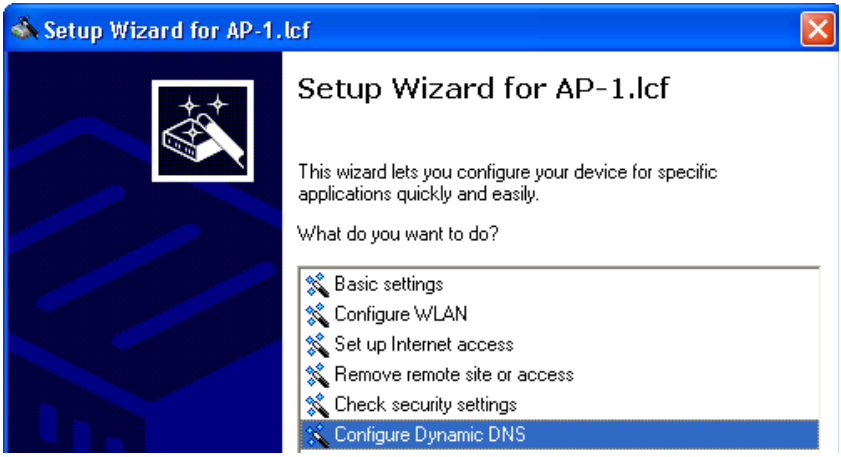
1: Server at DynDNS provider	3: OpenBAT Device
2: Internet	4: Client

An action is defined for this which, for example, automatically sends an http request to the DynDNS server each time a connection is established. The necessary information is transferred via the DynDNS account, thereby triggering an update of the registration. An http request of this type from DynDNS.org appears as follows:

```
http://Username:Password@members.dyndns.org/nic/
update?system=dyndns&hostname=%h&myip=%a
```

The host name of the action and the OpenBAT device's current IP address are sent to an account at DynDNS.org as specified by a username and password, and the appropriate entry is updated.

The settings necessary for this can be adjusted easily by using the Setup Wizard in LANconfig:


Setup Wizard for AP-1.lcf
Setup Wizard for AP-1.lcf
This wizard lets you configure your device for specific applications quickly and easily.
What do you want to do?
Basic settings
Configure WLAN
Set up Internet access
Remove remote site or access
Check security settings
Configure Dynamic DNS

The Setup Wizard supplements the basic action with further provider-specific parameters, which are not described here. Apart from that, the Setup Wizard creates additional actions that control the OpenBAT device in case the update does not succeed the first time.

Dynamic DNS client in the OpenBAT device via HTTP

As an alternative to using a simple http request to update DynDNS information, some services make use of the GnuDIP protocol. The GnuDIP protocol is based on a challenge-response mechanism, as follows:

- The client opens the connection to the GnuDIP server.
- The server responds with a random value calculated for the session.

- The client uses the random value and the password to create a hash value, and returns it to the server.
- The server checks this hash value and reports its result by sending a number back to the client.

The GnuDIP protocol can exchange messages between the client and server either via a simple TCP connection (standard port 3495) or as a CGI script running on an Internet server. The version using an http request from a CGI script has two advantages: no additional ports on the server need to be opened for GnuDIP, and HTTPS helps protect against passive interception and offline dictionary attacks.

Requests to a GnuDIP server are triggered by the OpenBAT device with an action in the following form:

```
gnudip://<srv>[:port][/path]?<parameter>
```

The elements of the GnuDIP request include:

- <srv> – The GnuDIP server address.
- [:port] – Specifying the port is optional. If it is not defined, default values are taken instead (3945 for TCP, 80 or 443 for http/https).
- [/path] – Path information alone is required by http/https to define the location where the CGI script is stored.

The following parameters are extensions to the request:

- method=<tcp|http|https> – Selects the protocol to be used for the transmission between the GnuDIP server and client. Just one protocol can be selected here.
- user=<username> – Specifies the user name for the account on the GnuDIP server.
- pass=<password> – Specifies the password for the account on the GnuDIP server.
- domn=<domain> – Specifies the DNS domain containing the DynDNS entry.

- reqc=<0|1|2> – Defines the action that is triggered by the request. Action <0> sends the server a dedicated IP address that is to be used for the update. Action <1> deletes a DynDNS entry. Action <2> triggers an update, although no IP address is transmitted to the server. Instead, the server carries out the update with the IP address of the GnuDIP client.
- addr=<address> – Specifies the IP address that an action with the parameter <0> is to use for updating the DynDNS entry. If this is unspecified in a <0> action, the request is treated as a <2> action.

With the GnuDIP protocol, the host name that is to be registered corresponds to the user name sent to the server. If, for example, the username is "myserver" and the DNS domain is "mydomain.org," then the DNS name "myserver.mydomain.org' is registered.

For example, the following action executed via the GnuDIP protocol updates the DynDNS entry at a DynDNS provider with the current IP address of the OpenBAT device (%a) as soon as a connection is established:

```
gnudip://gnudipsrv?method=tcp
&user=myserver&domn=mydomain.org
&pass=password&reqc=0&addr=%a
```

Use the following action to delete a DynDNS entry, for example once the connection has been terminated:

```
gnudip://gnudipsrv?method=tcp
&user=myserver&domn=mydomain.org
&pass=password&reqc=1&addr=%a
```

In response to the request, the GnuDIP server returns one of the following values to the GnuDIP client (assuming that the connection between server and client was established):

- 0 – The DynDNS entry was updated successfully.
- 0:address – The DynDNS entry was successfully updated with the specified address
- 1 – Authentication at the GnuDIP server was unsuccessful.
- 2 – The DynDNS entry was deleted successfully.

These responses can be evaluated by the OpenBAT device's actions to trigger further actions if necessary.

10.18.2 Action Examples

Broken Connection Alert as an SMS to a Mobile Telephone

The placeholder %t allows the current time of an event to be incorporated into a message. For example, an alert about the interruption of a WLAN connection can be sent by e-mail or as an SMS to a system administrator's mobile telephone.

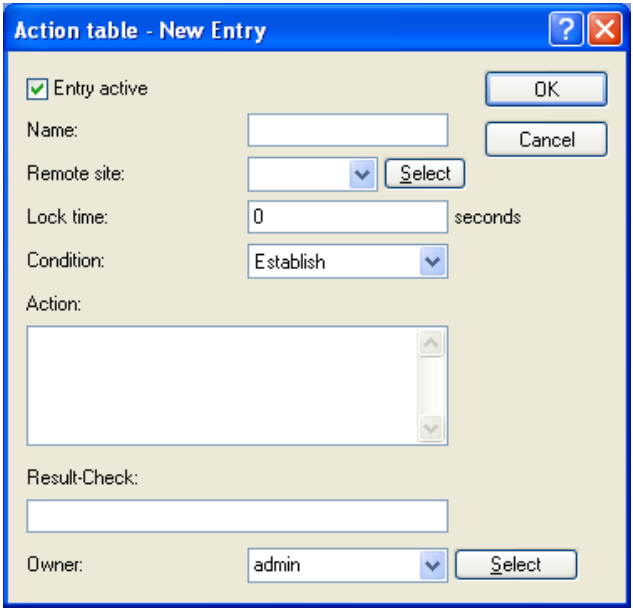
The following pre-conditions have to be met for messaging:

- The status of the WLAN connection is monitored, for example by means of "dead-peer-detection" (DPD).
- The OpenBAT device has to be configured as an NTP client in order to have the current system time.
- An SMTP account needs to be set up for transmitting e-mails.

After these requirements are met, messaging can be set up in the LANconfig software (for this example) by following these steps:

☐ Navigate to the following dialog:`Configuration : Communication : General` and click "Action table".

☐ Click "Add" to open the following dialog:



Configure the parameters in this dialog as follows:

- Name:
  Enter a name for the action.
- Remote site:
  Select the remote site.
- Lock time:
  Define an optional lock time to prevent the recurrence of this action for the specified time.
- Condition:
  Select ‘Broken’.
- Action:
  Configure the e-mail transmission, as follows:
  mailto:admin@mycompany.com?subject=WLAN connection broken at %t?body=WLAN
  connection to Subsidiary 1 was broken.

If the connection is broken, this action sends an e-mail to the administrator with the time of the event in the subject line.

Note:

- If the mail is sent to an appropriate Mail2SMS gateway the alert can be sent directly to a mobile telephone.
- For complex scenarios with several subsidiaries, each of the remote sites is given a corresponding entry in the central OpenBAT device. For monitoring the headquarters itself, an action is entered into a device at one of the branch offices. In this way the administrator receives an alert even if the WLAN gateway at the central location ceases to function.

Suppress Messaging in case of Re-connects with a DSL Connection

Some providers interrupt the DSL connection once every 24 hours. To avoid informing the administrator of these regular interruptions, messaging can be disabled at the time when the re-connect occurs.

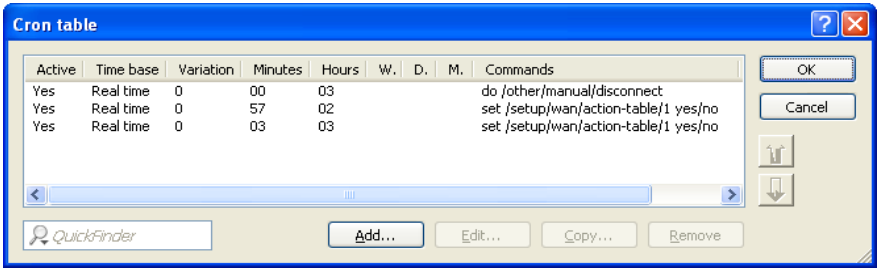
First of all an action is required to force the re-connect to occur at a fixed time; generally at night when the Internet connection is not in use. The entry defines, for example, 03:00h and the Internet connection is broken with the command:

```
do other/manual/disconnect internet
```

With two more Cron commands

```
set /setup/wan/action-table/1 yes/no
```

the corresponding entry in the action table is switched off three minutes before 03:00h and switched on again three minutes after 03:00h. The number 1 following the path to the action table is an index that stands for the first entry in the table.

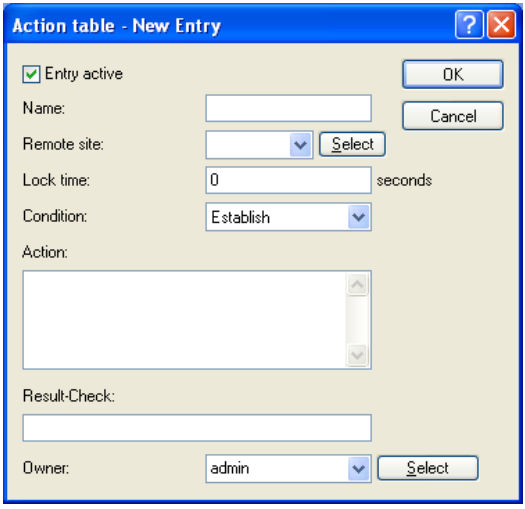


10.18.3Configuring action table entries

To configure entries for the Action table, follow these steps:

☐ Navigate to the following dialog:`Configuration : Communication : General` and click "Action table".

☐ Click "Add" to open the following dialog:



Configure the parameters in this dialog as follows:

- Enable:
  Activates or deactivates this entry.
- Name:
  The action name can be referenced in the fields ’Action’ and ’Check for’ with the place holder %h (host name).
- Remote site:
  A change in status of this remote site triggers the action defined in this entry.
- Lock time:
  Limits the repetition of this action within the period defined in seconds.

- Condition:
  The action is triggered when the change in WAN-connection status set here occurs. Possible values:
  - Establish: The action is triggered when the connection has been established successfully.
  - Disconnected without failure: The action is triggered when the device itself terminates the connection (e.g. by manual disconnection or when the hold time expires).
  - End (disconnected or broken): The action is triggered on disconnection (whatever the reason for this).
  - Broken with failure: This action is triggered on disconnects that were not initiated or expected by the device.
  - Establish failure: This action is triggered when a connection establishment was started but not successfully concluded.
- Action (max. 250 characters):
  Description of the action that should be executed when there is a change in the status of the WAN connection. Just one action can be triggered per entry. Possible values for the action includes:

  Note: For each of the following values, the colon (:) is part of the action value.

  - exec: This prefix initiates any command as it would be entered at the Telnet console. For example, the action “exec:do /o/m/d” terminates all current connections.
  - dnscheck: This prefix initiates a DSN name resolution. For example, the action “dnscheck:myserver.dyndns.org” requests the IP address of the indicated server.
  - http: This prefix initiates an http-get request. For example, you can use the following action to execute a DynDNS update at dyndns.org:
    http://username:password@members.dyndns.org/nic/update?system=dyndns&hostname=%h&myip=%a
    The meaning of the place holders %h and %a is described below.
  - https: Like “http:”, except that the connection is encrypted.

– gnudip: This prefix initiates a request to the corresponding DynDNS server via the GnuDIP protocol. For example, you can use the following action to use the GnuDIP protocol to execute a DynDNS update at a DynDNS provider:
gnudip://
gnudipsrv?method=tcp&user=myserver&domn=mydomain.org&pass=password&reqc=0&addr=%a
The meaning of the place holder %a is described below.

– repeat: This prefix together with a time in seconds repeats all actions with the condition 'Establish' as soon as the connection has been established. For example, the action 'repeat:300' causes all of the establish actions to be repeated every 5 minutes.

– mailto: – This prefix causes an e-mail to be sent. For example, you can use the following action to send an e-mail to the system administrator when a connection is terminated:
mailto:admin@mycompany.de?subject=WLAN connection broken at %t?body=WLAN connection to Branch Office 1 was terminated.
With the extension of attachments in e-mails, there can be done any console commands on the device and the result will be sent as attachment in an e-mail. In this way, the content of tables or menus (e.g. detailed status messages) can be sent by e-mail.

Optional variables for the actions include:

– %a – WAN IP address of the WAN connection relating to the action.

– %H – Host name of the WAN connection relating to the action

– %h – Like %H, except the hostname is in small letters

– %c – Connection name of the WAN connection relating to the action.

– %n – Device name

– %s – Device serial number

– %m – Device MAC address (as in Sysinfo)

– %t – Time and date in the format YYYY-MM-DD hh:mm:ss

– %e – Description of the message that was reported when connection was not established

- Result-Check:
  The result of the action can be evaluated here to determine the number of lines to be skipped in the processing of the action table. Possible values:
  - contains=
    This prefix checks if the result of the action contains the defined string.
  - isequal=
    This prefix checks if the result of the action is exactly equal to the defined string.
  - ?skipiftrue=
    This suffix skips the defined number of lines in the list of actions if the result of the 'contains' or 'isequal' query is TRUE.
  - ?skipiffalse=
    This suffix skips the defined number of lines in the list of actions if the result of the 'contains' or 'isequal' query is FALSE.

  Optional variables for the actions are the same as those for the Action, above.
- Owner:
  The exec actions are executed with the rights of the owner. If the owner does not have the necessary rights (e.g. administrators with write access) then the action will not be executed.

10.19 Using the LAN Serial Interface

In the IT field, COM port servers—also known as serial port servers—are devices that transport data between TCP and serial connections. There are many applications:

- Networking of devices with a serial interface but without a network interface.
- Remote maintenance of devices that can be configured only a a serial interface.
- Virtual extension of a serial connection between two devices with serial interfaces over a network.

Most OpenBAT devices feature a serial interface that can be used to carry out configurations or to connect to a modem. In some cases the interface is used for neither of these purposes, yet a COM port server is required in the vicinity of the device. In this case, the OpenBAT device can use its serial interface as a COM port server, thereby saving the cost of an external COM port server. If the OpenBAT device is used in an application that focuses on the serial configuration interfaces of other devices, additional serial interfaces can be provided by some models by employing suitable CardBus or USB adapters. This design enables multiple instances of the COM port server to operate in a single OpenBAT device.

10.19.1 Operating Modes

A COM port server has two operating modes:

- Server mode: The COM port server waits for requests from a defined TCP port to establish TCP connections. The mode can be used for remote maintenance, for example.
- Client mode: As soon as a device connected to the serial interface becomes active, the COM port client opens a TCP connection to a preset remote site. This operating mode is used, for example, for devices that have just one serial interface but require network access.

In both of these cases, a transparent connection is established between the serial interface and the TCP connection. Data packets received at the serial interface are forwarded to the TCP connection, and vice versa.

A common server-mode application is to install a virtual COM port driver at the remote site that connects to the COM port server. Drivers of this type allow applications running at the remote site to use the TCP connection as if it were an additional COM port. The IETF RFC 2217 standard describes the Telnet WILL/DO protocol extensions, which transmit the negotiations for the serial connection (bitrate, data and stop bits, handshake) to the COM port server. The use of this protocol is optional, so practical default values can be set in the COM port server.

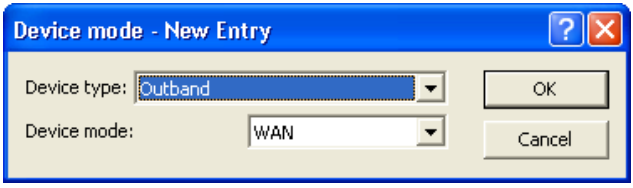
10.19.2 Configuring the Serial Interface

The "Device mode" table allows individual serial devices to be assigned to specific applications. When the device recognizes a hot-pluggable USB adapter, the device automatically creates a new entry for provided serial interfaces in this table. This automatic operation facilitates the configuration of the serial devices The built-in serial interface of the OpenBAT device is an exception; you must configure it manually.

To manually configure an entry for the Devices table, follow these steps:

☐ Navigate to the following dialog:`Configuration : COM Ports : Devices` and click "Device mode".

☐ In the ‘Device mode’ table, click ‘Add...’ to open the ‘New Entry’ dialog:



Select settings for the following parameters:

- Device type:
  The serial interface from the list of those available in the device.
- Device mode:
  The operating mode for the device. Values include:
  - WAN: The device ports can be used for operating a modem. The operating mode sets the device ports to serial interfaces.
  - COM port server: The outband interface can be used for device management.

  Note: Some devices support ‘COM port server’ device operating mode.

10.19.3Configuring the COM Port Server

Configuring the COM port server involves making entries in three tables:

- Device ports table
- Serial interface table
- Network interface table

What all three tables have in common is that a certain port at a serial interface is identified by the values for device type and port number. Because some serial devices such as a CardBus card have multiple ports, the port to be used needs to be specified explicitly. For a device with just one port, for example, a single serial configuration interface, the port number is set to zero.

Device Ports Table: Operational Settings

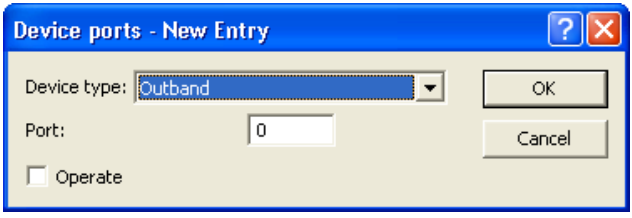
This table activates the COM port server at a port of a specified serial interface. Add an entry to this table to start a new instance of the COM port server. Delete an entry to delete the corresponding server instance. The switch Operating can be used to deactivate a server instance in the table.

When a server instance is created or activated, the other tables in the COM port configuration are searched for matching device type and port number values. If no suitable entry is found, the server instance takes workable default values.

To manually configure an entry for the Device Ports table, follow these steps:

☐ Navigate to the following dialog:`Configuration : COM Ports : Server` and click "Device ports".

☐ In the ‘Device ports’ table, click ‘Add...’ to open the ‘New Entry’ dialog:



Enter settings for the following parameters:

- Device type:
  The serial interface from the list of those available in the device.
- Port:
  Some serial devices such as the CardBus have more than one serial port. Enter the number of the port on the serial interface that is to be used for the COM-port server.
- Operate:
  Enables and disables the COM port server on the selected port of the selected interface.

Serial interface table: COM port settings

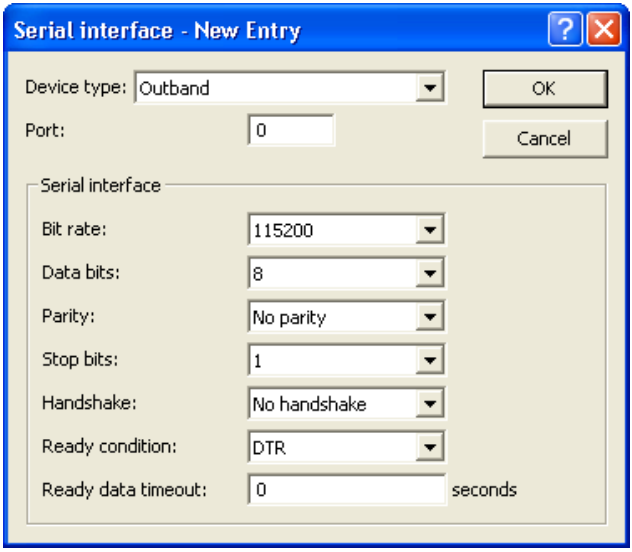
This table contains the settings for data transmission over the serial interface.

Note: All of these parameters can be overwritten by the remote site if the RFC2217 negotiation is active. Current settings can be viewed in the status menu in WEBconfig.

To manually configure an entry for the Serial Interface table, follow these steps:

☐ Navigate to the following dialog:`Configuration : COM Ports : Server` and click "Serial interface".

☐ In the ‘Serial interface’ table, click ‘Add...’ to open the ‘New Entry’ dialog:



Enter settings for the following parameters:

- Device type:
  The serial interface from the list of those available in the device.
- Port:
  Some serial devices such as the CardBus have more than one serial port. Enter the number of the port on the serial interface that is to be used for the COM-port server.
- Bit rate:
  Bitrate used on the COM port. Values range from 110 to 230400 Bps.
- Data bits:
  Number of data bits—7 or 8.
- Parity:
  The checking technique used on the COM port. Values include no parity, odd or even.
- Stop bits:
  The number of stop bits—1 or 2.
- Handshake:
  The data-flow control used on the COM port—RTS/CTS (flow control) or no handshake.

- Ready conditions:
  A characteristic of a serial interface is the ready state. The COM port server does not forward data from serial to network side, unless it is in ready state. Furthermore the change-over from ready- to not-ready state in operating mode 'client' (which has to be set in the network table), is used for establishing/terminating a TCP connection. Currently there are two alternatives to recognize the ready state of the serial interface. This can be set using the parameter Ready condition.
  - DTR mode (default): The handshake line is monitored. The serial interface is regarded as ready, as long the DTR line is active.
  - Data mode: The ready state is expected after characters are received on the serial interface.

  If there are no characters received for the period of time set in Ready data timeout, the state falls back to 'not ready'. This mechanism can be switched off by setting the timeout value to 0. The serial interface is ready, if the ready condition option is set to ‘data’ and the timeout is set to ‘zero’.
- Ready data timeout:
  The timeout switches the port back to the not-ready status if data is not received within this time period. This function is deactivated when timeout is set to zero. In this case the port is ready if the data mode is selected.

Network interface table: Network settings

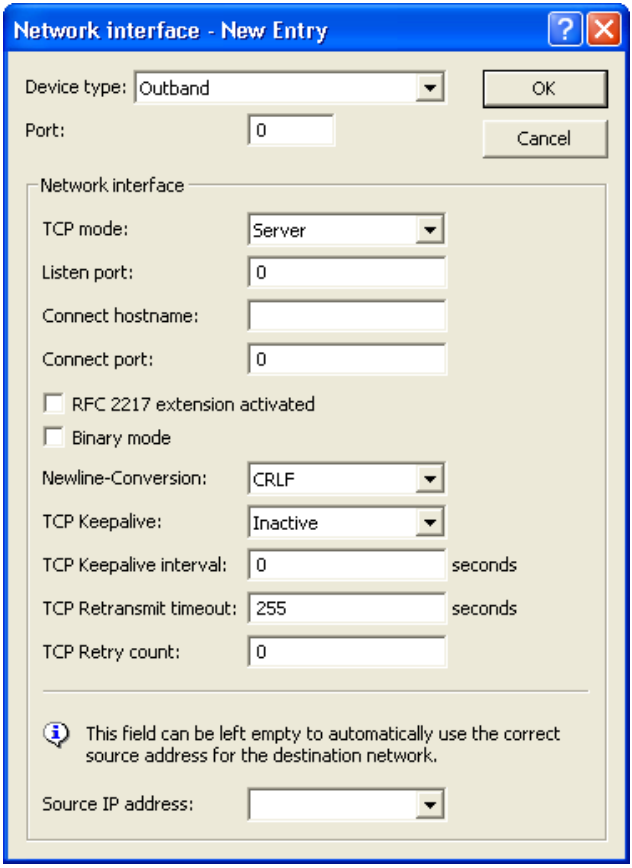
This table contains all settings that define the behavior of the COM port in the network.

Note: All of these parameters can be overwritten by the remote site if the RFC2217 negotiation is active. Current settings can be viewed in the status menu in WEBconfig.

To manually configure an entry for the Network Interface table, follow these steps:

☐ Navigate to the following dialog:`Configuration : COM Ports : Server` and click "Network interface".

☐ In the ‘Network interface’ table, click ‘Add...’ to open the ‘New Entry’ dialog:



Enter settings for the following parameters:

- Device type:
  The serial interface from the list of those available in the device.
- Port:
  some serial devices such as a CardBus have more than one serial port. In this case, enter the number of the port that the COM port server uses on the serial interface

- TCP mode:
  Select a mode:
  - Server mode: Each instance of the COM port monitors the specified listen port for incoming TCP connections. Just one active connection is permitted per instance. All other connection requests are refused.
  - Client Mode: The instance attempts to establish a TCP connection via a defined port to the specified remote site, as soon as the port is ready. The TCP connection is closed again as soon as the port becomes unavailable.

  In each case, a OpenBAT device closes any open connections when the device is restarted.
- Listen port:
  The TCP port where the COM port in TCP server mode expects incoming connections.
- Connect hostname:
  The COM port in TCP client mode establishes a connection to this host as soon as the port is in "Ready" status.
- Connect port:
  The COM port in TCP client mode uses this TCP port to establish a connection as soon as the port is in "Ready" state.
- RFC 2217 extension activated:
  The RFC2217 extensions can be activated for both TCP modes. With these extensions activated, the OpenBAT device uses the IAC DO COM-PORT-OPTION sequence to signal that it will accept Telnet control sequences. The COM port subsequently works with the corresponding options; the configured default values are overwritten. The port also attempts to negotiate the local echo and line mode for Telnet. Using the RFC2217 extensions with incompatible remote sites is not recommended. Unexpected characters may be displayed at the remote site. A side effect of using the RFC2217 extensions may be that the port regularly carries out an alive check as Telnet NOPs are transmitted to the remote site.
- Binary mode:
  Serial data will be forwarded as binary. Thereby no CR/LF (Carriage Return / Line Feed) conversion occurs.

- Newline conversion:
  This defines which character sequence is sent to the serial port if a newline character is received in non-binary mode. The default setting (CRLF) will reproduce what was received over the TCP connection, but it is not necessarily the correct setting for all applications. For instance, some Unix serial consoles will interpret this sequence as an undesirable double linefeed, so a single linefeed or carriage return is more appropriate. If another LANconfig device's outbound port is attached to the serial port, either CRLF or CR will do, but not LF because carriage return characters are expected by a LANconfig for its auto-bauding feature.
- TCP Keepalive:
  When active, the TCP implementation will regularly send certain dummy packets to the remote site. These packets contain no payload data, but hinder firewalls and NAT gateways from discarding this connection since the connection still looks alive. In extension to RFC 1122, the TCP keepalive offers three modes of operation:
  - Inactive: No packets are sent during idle periods.
  - Active: Packets are regularly sent, but the lack of answers to these packets has no further effect. Connection entries in firewalls or NAT gateways will be kept alive, but the complete loss of the TCP connection will not be detected. This mode of operation is recommended for server operation.
  - Proactive: The TCP stack additionally expects answers to its keepalive packets and will report a broken TCP connection in case no answer is received after several attempts. The number of tries is the same as the "TCP Retry count" for data packets (see below).
- TCP Keepalive interval:
  Defines how often the TCP stack will transmit keepalive packets. A setting of 0 results in the internal default of 7200 seconds.
- TCP Retransmit timeout:
  Specifies the time after which a single retransmission is started. A value of 0 is equal to the default value (60 seconds). Note that the actual time until a connection is detected as broken is the sum of all retransmissions.

- TCP Retry count:
  This limits the total number of retransmits. A retry count of zero is equal to setting the default value of 5 retries.
- Source IP address:
  An optional source address can be configured here. This address is used instead of the source address, which is otherwise obtained automatically for the respective destination address. When loopback addresses are configured, they can be input here.

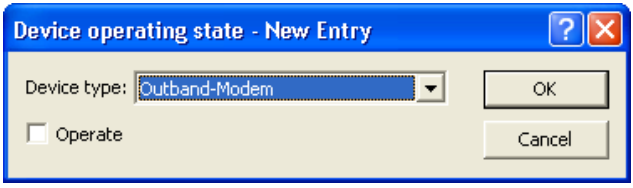
10.19.4WAN Device Configuration

The table with WAN devices is a status table. All HotPlug devices (connected via USB or CardBus) are automatically entered into this table.

To manually configure an entry for the Devices table, follow these steps:

☐ Navigate to the following dialog:`Configuration : COM Ports : WAN` and click "Device operating state".

☐ In the ‘Device operating state’ table, click ‘Add...’ to open the ‘New Entry’ dialog:



Select settings for the following parameters:

- **Device type:**
  The serial interface from the list of those available in the device.
- **Operate:**
  Enabled/disabled status of the device.

10.19.5 Serial Connection Status Information

Various statistics and status values are recorded for every instance of the COM-port server. This includes data relating to:

- Network status
- COM port status
- Byte counters
- Serial port errors
- Connections

In addition, you can clear the content of all status tables.

All this data is available in Telnet. Navigate in WEBconfig to the following place:

`HiLCOS Menu tree: Status : COM Ports`

Network Status

This table contains information on current and recent TCP connections. Field values include:

- Device type:
  List of serial interfaces available in the device.
- Port number:
  The port number used for the COM port server on the serial interface.
- Connection status:
  Possible values include:
  - Connected: An active connection exists (server or client mode).
  - Listening: This instance is working in server mode; no TCP connection is currently active.
  - Not listening: In server mode, the specified TCP port could not be reserved for inbound connections, e.g. because it is already occupied by another application.

  - Blank: This instance is working in client mode and the port is not ready. No TCP connection will be established now.
  - Transfer: The port has reached the 'ready' state; a connection is being established.

- Last error:
  In client mode this displays the reason for the last unsuccessful connection attempt. In server mode this value has no significance.
- Remote address:
  Displays the IP address of the remote site for a successful TCP connection.
- Local port:
  Displays the local TCP port used for a successful TCP connection.
- Remote port:
  Displays the remote TCP port used for a successful TCP connection.

COM Port Status

This table displays the serial port status and the settings currently used by this port.

- Device type: List of serial interfaces available in the device.
- Port number: The port number used for the COM port server on the serial interface.
- Port status: Possible values:
  - Not available: The serial port is currently not available to the COM port server, for example because the USB or CardBus adapter has been removed or because it is being used by other functions in the OpenBAT device.
  - Not ready: The serial port is available to the COM port server but is currently not ready for data transfer, for example because the DTR line is inactive. In the client state, no attempt is made to establish a connection as long as the port is in this state.
  - Ready: The serial port is available and ready for data transfer. In the client state, no attempt is made to establish a connection as long as the port is in this state.

Note: The port status is relevant in server mode, too. All TCP connection requests are accepted, although the COM port instance transfers data exclusively between the serial port and the network when the serial port has reached the "ready" state. The following columns display the settings that are currently in use on the serial port. These are either the values as configured or as set by the negotiations via the RFC2217 extensions.

- Bit rate: Bit rate used on the COM port.
- Data bits: Number of data bits.
- Parity: The checking technique used on the COM port.
- Stop bits: Number of stop bits.
- Handshake: The data-flow control used on the COM port.

Byte Counters

This table displays the inbound and outbound data packets at the serial port and on the network side.

Note: These values are not reset when the connection is opened or closed.

- Device type: List of serial interfaces available in the device.
- Port number: The port number used for the COM port server on the serial interface.
- Serial-Tx: Number of bytes sent over the serial interface.
- Serial-Rx: Number of bytes received over the serial interface.
- Network-Tx: Number of bytes sent to the network.
- Network-Rx: Number of bytes received from the network.

COM Port Errors

This table displays the anomalies on the serial port. These messages may indicate a broken cable or incorrect parameter settings in the configuration.

- Device type: List of serial interfaces available in the device.
- Port number: The port number used for the COM port server on the serial interface.
- Parity errors: A count of events caused by a checksum mismatch.
- Framing errors: Number of corrupted data packets.
- Rx Lost errors: The number of lost transmissions.

Connections

This table displays successful and unsuccessful TCP connections in both server mode and client mode.

- Device type: List of serial interfaces available in the device.
- Port number: The port number used for the COM port server on the serial interface.
- Server granted: Number of connections granted by the COM port server.
- Server rejected: Number of connections rejected by the COM port server.
- Client succeeded: Number of connections successfully established by the COM port client.
- Client DNS error: Number of connections that the COM port client could not establish due to DNS reasons.
- Client TCP error: Number of connections that the COM port client could not establish due to TCP reasons.
- Client remote disconnects: Number of connections where the COM port was disconnected from the remote site.

- **Delete Values**

  This action deletes all values in the status tables.

10.19.6CPM Port Adapters

Devices with serial interfaces can be connected to a OpenBAT device in the following ways:

Adapters	OpenBATs
COM-port adapters	All those with a serial configuration interface
USB serial adapter	All those with a USB interface
CardBus serial adapter	All those with a CardBus slot
Modem adapter	All those with a serial configuration interface

The COM port adapter needs to be a two-way D-sub plug with the following PIN assignment:

Pin	Signal	Signal	Pin
2	RxD	TxD	3
3	TxD	RxD	2
4	DTR	DSR	6
5	GND	GND	5
6	DSR	DTR	4
7	RTS	CTS	8
8	CTS	RTS	7

10.20IGMP Snooping

10.20.1Introduction

All OpenBAT devices feature a "LAN bridge," a software mechanism for transferring data between the Ethernet ports and the WLAN interfaces. In many ways the LAN bridge works like a switch. The core task of a switch, as opposed to a hub, is to forward packets to the specific port to which the relevant user is connected. Based on the incoming data packets, the switch automatically creates a table listing the senders' MAC addresses and their ports.

If the table contains the destination address for an incoming packet, the switch forwards the packet to the corresponding port. If the destination address is not in the table, the switch forwards the packet to all ports. That is to say, a switch can deliver a packet precisely provided that the destination address appeared earlier in a packet arriving at a certain port from the sender's address. However, broadcast or multicast packets can never be entered as a sender address into a packet, and so these packets end up being flooded to all ports.

This may be the correct action for broadcasts that are supposed to reach all available recipients, but it may not be the case for multicasts. Multicasts are usually aimed at a targeted group of recipients within a network, but not all of them. Example:

- Video streams are frequently transmitted as multicasts, but not all of the network stations are intended to receive that stream.
- Various applications in the medical field use multicasts to send data to certain terminal devices, but this data should not be available to all stations.

A LAN bridge in the OpenBAT device will have ports to which no multicast recipients are connected. While this "unnecessary" transmission of multicasts to ports without any receivers is not an error, it can impact overall performance:

- Many stations are unable to reject the unwanted multicasts in their hardware. Instead, the packets are forwarded to higher protocol layers, which leads to an increase in CPU load.
- WLANs are particularly susceptible to bandwidth restrictions due to multicasts if none of the associated WLAN clients want to receive the multicast.

The TCP/IP protocol suite defines the Internet Group Management Protocol (IGMP) that network stations can use to notify their router of their intention to receive certain IP multicasts. Stations carry out a multicast registration with their router to subscribe to certain multicast groups which deliver the relevant packets. IGMP makes use of "Join" messages and "Leave" messages to register and un-register as a multicast group member.

Note: Information describing which multicast groups a station can or should join is available from protocols other than IGMP.

As a layer-3 protocol, IGMP performs multicast guiding/routing for entire IP subnets. However, network devices such as bridges, switches or WLAN access points forward the packets exclusively via layer 2, meaning that IGMP itself does not help to further guide multicast traffic through this substructure. For this reason, the bridges use the multicast registrations between stations and routers to receive additional information for targeting the distribution of multicasts. IP multicasts merely need to be forwarded to an interface where a router is located that is capable of multicast routing, and therefore of forwarding multicasts to other IP subnets. This method is called IGMP snooping. The bridges, which normally use the MAC on layer 2 for packet forwarding, thus additionally use the layer 3 information in the IP multicast packets.

For more detailed description of the functions of IGMP snooping in a OpenBAT device, understand the following terms:

- A port is a "member" of a multicast group if at least one station connected to it wishes to receive the packets for a certain multicast address. Multicast registration can be dynamic via IGMP snooping or configured manually.
- A port is a "router port' if it is connected to a router that is capable of multicast routing and therefore of forwarding multicasts to other IP subnets.
- A multicast group is "unregistered" if none of the interfaces attached to the bridge is a member of this multicast group.

10.20.2IGMP Snooping Operation

Whenever a packet is received, the bridge initially determines whether it is a unicast, broadcast, or multicast packet. For broadcast and unicast packets, the bridge operates in the usual way, i.e. it floods to all ports or sends to a specific port based on the MAC table entry for the recipient.

Two types of IP multicast packet are differentiated (whereby packets which are truncated or contain an invalid checksum are discarded entirely):

- IGMP messages are handled in different ways depending on their content:
  - A 'Join' message results in the incoming port becoming a member of the respective multicast group. This message is forwarded to router ports exclusively.
  - Similarly, a 'Leave message' results in the incoming port being removed from the multicast group's member list. This message is also forwarded to router ports exclusively.

- An incoming IGMP query results in the port being marked as a router port. These messages are flooded to all interfaces.
- All other messages are flooded to all interfaces—no ports experience a change of state.

- If an IP multicast packet does not contain an IGMP message, the IP destination address is examined. Packets for the destination address ‘224.0.0.x’ are flooded to all ports because this is a ‘reserved’ range. For all other packets the destination address is looked up in the IGMP membership table:
  - If the address is found, the packet is forwarded according to the membership stored in the table.
  - If the address is not found, the packet may either be discarded, flooded to all ports, or forwarded exclusively to all router ports (depending on the configuration).

10.20.3IGMP snooping through multiple bridges

As described, IGMP snooping forwards incoming ‘Join’ or ‘Leave’ messages via router ports. In a structure with multiple bridges, initially none of the ports are router ports or members of a multicast group. If a station connected to the bridge registers with a multicast group, the port automatically becomes a member of this group. However, none of the ports are router ports at this point, so the ‘Join’ messages are not forwarded anywhere. Other bridges thus receive no information about the port's membership with the multicast group.

Consequently, bridges need to be equipped with router ports in order for membership information to be propagated. Because the ports of a bridge become router ports only in the case of IGMP queries, one of the multicast-capable routers in the network needs to take over the task of distributing the necessary IGMP queries throughout the network. This router is referred to as the IGMP querier. If the network does not contain a multicast router, the

OpenBAT access points are capable of simulating a querier. To avoid parallel queries arriving from various queriers, a querier will deactivate itself if it discovers another querier with a lower IP number. The distribution of IGMP information by the querier can be explained with the following example:

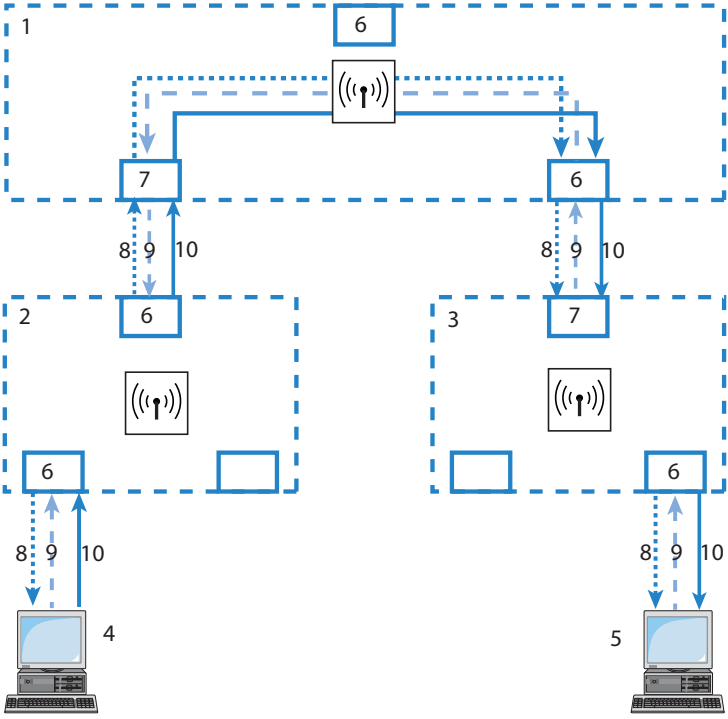


Figure 122:IGMP snooping through multiple bridges

1: Bridge 1	6: Member port
2: Bridge 2	7: Router port
3: Bridge 3	8: Query
4: PC-1	9: Join
5: PC-2	10: Data

- The querier (Bridge 2 in this example) regularly sends out IGMP queries on all ports of bridge 2 (dotted lines). The next bridge (Bridge 1) receives the query on a port which is then marked as a router port (R). PC 1 responds to this query with a Join message for all multicast groups (light dashed lines) that it wishes to join. The port connecting PC 1 to Bridge 2 then becomes a member of the multicasting group(s).
- In addition to this, Bridge 1 sends the queries on all other ports to the bridges and stations lower down in the structure. In Bridge 3 the port receiving the query becomes a router port (R).
- The station (PC 2) connected to bridge 3 responds to this query with a Join message for all registered multicast groups. The port connecting PC 2 to Bridge 3 then becomes a member of the multicasting group(s).
- Bridge 3 forwards this Join message to Bridge 1 over the router port. The receiving port on Bridge 1 thus also takes on membership of the multicast groups that PC 2 has registered for.
- In the final step, Bridge 1 forwards the Join message from PC 2 via the router port to Bridge 2, where the receiving port also takes on membership of PC 2's multicast groups.

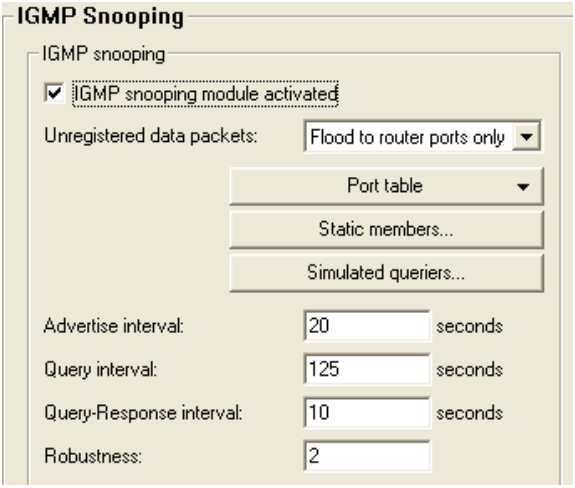
If PC 1 now transmits a multicast for which PC 2 has registered, all of the bridges (2, 1 and then 3) forward the packets to PC 2 via the member port.

10.20.4 Configuring IGMP Snooping

General Settings

To configure general IGMP settings in LANconfig, follow these steps:

☐ Open `Configuration : Interfaces : IGMP Snooping`:



Enter settings for the following IGMP general properties:

- IGMP snooping module activated:
  This enables or disables the IGMP snooping function, plus any configured IGMP querier entities that might have been defined.
  - If enabled: the LAN bridge will track any IGMP traffic and sort ports for IGMP relevance.
  - If disabled: the LAN bridge will behave like a 'dumb switch' and flood all IP multicasts to all ports.

  A change of this setting will implicitly reset the snooping engine to its initial state, i.e. all port properties learned dynamically (memberships, router port properties) will be cleared.
- Unregistered data packets:
  This setting defines the handling of multicast data packets with a destination address outside the 224.0.0.x range and no defined memberships (i.e. no static members were defined, and no dynamic memberships were learned by the reception of IGMP join messages). Values include:
  - Router ports only (default): Sends these packets to all router ports.
  - Flood: Sends these packets to all ports.
  - Discard: Drops these packets.
- Advertise interval:
  The interval during which devices send packets advertising themselves as multicast routers. This information makes it quicker for other IGMP-snooping devices to find which of their ports are to operate as router ports. When activating its ports, a switch (for example) can query for multicast routers, and the router can respond to this query with an advertisement of this type. Under some circumstances this method can be much quicker than the alternative IGMP queries. Values are in seconds, and range from 4 to 180. The default is 20 seconds.

- Query interval:
  Interval in seconds during which a multicast-capable router (or a simulated querier) sends IGMP queries to the multicast address 224.0.0.1, prompting the stations to transmit return messages regarding multicast group memberships. These regular queries influence the time in which memberships age, expire, and are then deleted, as follows:
  - After the startup phase, the querier sends IGMP queries in this interval.
  - A querier returns to the querier status after a time equal to: Robustness * Query Interval + ((Query-Response Interval) / 2).
  - A port loses its router-port status after a time equal to: Robustness * Query Interval + ((Query-Response Interval) / 2).

  Values: a 10-figure number greater than 0. Default = 125.
- Query-Response interval:
  This Interval, in seconds.
  - influences the timing between IGMP queries and router-port aging and/or memberships.
  - is the time period during which a multicast-capable router (or a simulated querier) expects to receive responses to its IGMP queries. These regular queries influence the time in which memberships age, expire, and are then deleted.

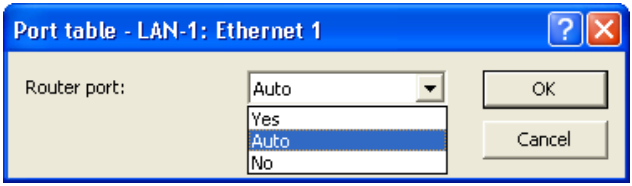
  Values: a 10-figure number greater than 0. Default = 10.
- Robustness:
  This setting tolerates packet losses of IGMP queries with respect to ‘Join’ messages. Possible values include a 10-figure number greater than 0. A value of 1 is not recommended. Default = 2.

Port Settings

To configure IGMP port settings in LANconfig, follow these steps:

☐ Open `Configuration : Interfaces : IGMP Snooping`.

☐ Click ‘Port table’, then select a port from the list to open the following dialog:



Enter settings for the following IGMP port properties:

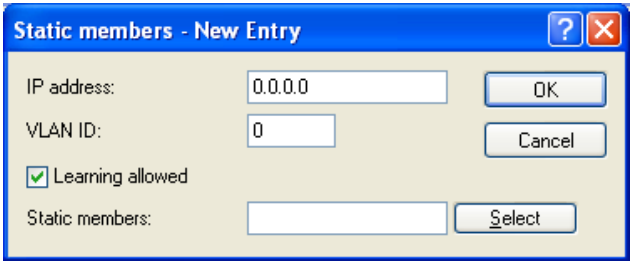
- **Router port:**
  This option defines the port's behavior. Selections include:
  - Yes: This port will serve as a router port, irrespective of IGMP queries or router messages received at this port.
  - Auto (default): This port will serve as a router port if IGMP queries or router messages are received. The port loses this status if no packets are received for a time duration equal to: Robustness*Query-Interval+(Query-Response-Interval/2).
  - No: This port will not serve as a router port, irrespective of IGMP queries or router messages received at this port.

Static Members

To configure IGMP static member settings in LANconfig, follow these steps:

☐ Open `Configuration : Interfaces : IGMP Snooping` and click ‘Static members’.

☐ In the ‘Static members’ table, click ‘Add...’ to open the ‘New Entry’ dialog:



Enter settings for the following IGMP static members properties:

- IP address:
  The IP address of the manually defined multicast group.
- VLAN ID:
  The VLAN ID which is to support this static member. Each IP multicast address can have multiple entries with different VLAN IDs. Possible values: 0 to 4096 default = 0.

  Note: If ‘0’ is selected, the IGMP queries are sent without a VLAN tag. For this reason, this value makes sense when VLAN is deactivated in general.

- Learning allowed:
  This option activates the automatic learning of memberships in this multicast group. If automatic learning is deactivated, packets can only be sent via the ports which have been manually defined for the multicast group.
- Static members:
  These ports will continue to serve as the destination for packets with the corresponding IP multicast address, irrespective of any Join messages received. Enter values in the form of a comma-separated list of the desired ports, up to a maximum of 215 alphanumerical characters.

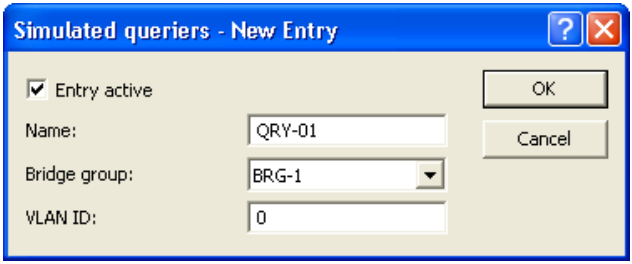
Simulated Queriers

This table contains all of the simulated queriers defined in the device. These units are employed if IGMP functions are required but there is no multicast router in the network. The querier can be limited to certain bridge groups or VLANs by defining multiple independent queriers to support the corresponding VLAN IDs.

To configure IGMP simulated queriers in LANconfig, follow these steps:

☐ Open `Configuration : Interfaces : IGMP Snooping` and click ‘Simulated queriers’.

☐ In the ‘Simulated queriers’ table, click ‘Add...’ to open the ‘New Entry’ dialog:



Enter settings for the following IGMP simulated querier properties:

- Entry active:
  Activates or deactivates the querier instance.
- Name:
  Name of the querier instance, containing up to 8 alpha-numeric characters.
- Bridge group:
  Limits the querier instance to a certain bridge group. If bridge group is set to ‘none’, the IGMP queries will be sent via all bridge groups.
- VLAN ID:
  An entry limits the querier instance to the specified VLAN. Because this parameter is also an index field, it is possible to make definitions that differ in the VLAN ID. A valid VLAN ID is in the range of 0...4094. The value 0 is meaningful if the VLAN module is turned off and then refers to untagged frames.

10.20.5IGMP Status

IGMP snooping status messages can be viewed in WEBconfig for the following:

- General status
- Groups status

- Port Status
- Simulated queriers

In addition, you can clear the content of all status tables.

These messages are presented in WEBconfig at:

```
HiLCOS Menu Tree : Status : LAN
BridgeStatistics : IGMP Snooping
```

General Statistics

This table contains information on IGMP packets. Field values include:

- Bad packets:
  The number of damaged data or IGMP packets received at all ports. Possible causes for damage to packets may be IP checksum events or truncated packets.

  Note: For performance reasons, IP checksums are evaluated just for IGMP packets, and not for the data portion of multicast packets. Hence, packets with an inaccurate checksum in the TCP/UDP or IP header are not detected. These packets are counted as data packets.

- Control packets:
  The number of intact IGMP packets received at all ports.
- Data packets:
  The number of intact IPv4 multicast packets received at all ports that are not IGMP packets.
- IPv4 Packets:
  The number of IPv4 multicast packets received at all ports, whether they were IGMP packets or not.
- Operating:
  Indicates whether IGMP snooping is activated or deactivated.

Groups Status

This table displays all the multicast group memberships known to the device, irrespective of whether they were configured statically or learned dynamically. If both static and dynamic memberships exist for a multicast group, these are shown in separate entries. Field values include:

- Address: The group's IP multicast address.
- VLAN ID: The VLAN ID to which this entry applies.
- Allow learning:
  Indicates whether new memberships for this group can be learned dynamically.
- Static members:
  The list of statically defined members for this group.
- Dynamic members:
  The list of dynamically learned members for this group.

Port Status

This table displays all port related statistics. Field values include:

- Router port:
  Indicates whether the port is currently in use as a router port, irrespective of whether this status was configured statically or learned dynamically.
- IPv4 packets:
  The number of IPv4 multicast packets received at this port, whether they were IGMP packets or not.
- Data packets:
  The number of intact IPv4 multicast packets received at this port that are other than IGMP packets.
- Control packets:
  The number of intact IGMP packets received at this port.
- Bad packets:
  The number of damaged data or IGMP packets received at this port. Possible causes for damage to packets may be IP checksum events or truncated packets.

Note: For performance reasons, IP checksums are evaluated just for IGMP packets, and not for the data portion of multicast packets. Hence, packets with an inaccurate checksum in the TCP/UDP or IP header are not detected. These packets are counted as data packets.

Simulated Queriers

This table shows the status of all defined and active IGMP querier instances. Field values include:

- Name:The name of the multicast group.
- Bridge group: The bridge to which this entry applies.
- VLAN ID: The VLAN to which this entry applies.
- Status: The current status of the entry:
  - Initial: The querier instance has just started and is sending IGMP queries in short intervals (four-times faster than the query interval defined).
  - Querier: The querier instance considers itself to be the active querier and is sending IGMP queries in the defined query interval.
  - Non-Querier: Another querier instance with a lower IP address has been detected, and the instance listed here is not sending any IGMP queries.

11 Configuring the Firewall

In an industrial environment, a firewall is indispensable for the separation of subnets, or for securing the LAN if the Internet access is also provided. But each connection from a workstation on the local network to the Internet represents a potential entry point for unauthorized users, who may attempt to access and edit your data, and manipulate your device configurations.

11.1 The Device Firewall

This chapter introduces the firewall embedded in the OpenBAT device.

Note: For ease of understanding, this chapter uses IPv4 as a basis for explanation and is mainly confined to the general firewall settings and the IPv4-specific configuration. Detailed documentation and background information on the IPv6 firewall is available separately in the chapter IPv6 (see on page 752).

11.1.1 Tips for Configuring the Firewall

The firewall in the OpenBATdevice is an extremely flexible and powerful tool. The following advice is offered to help you create rules for your firewall.

Default Firewall Settings

On delivery there is exactly one entry in the Firewall rule table: 'WINS'. This rule inhibits unwanted connection set-ups on the default route (usually to the Internet) by the NetBIOS protocol. Windows networks send inquiries in regular intervals into the network to find out if known stations are still available. This leads, in the case of a time-based account of network coupling, to unwanted connection set-ups.

Note: The OpenBAT device can prevent this, using the integrated NETBIOS proxy for network couplings, by simulating an answer for the concerned resource, until a real access takes place.

Security by NAT and Stateful Inspection

If no further firewall rule will be entered, the local area network benefits from the interaction of Network Address Translation (NAT) and stateful inspection. Only connections from the local area network produce an entry in the NAT table, whereupon the OpenBAT device opens a communication port. The stateful inspection monitors the communication via this port. Packets that belong to this connection may communicate via this port. For attempted access from the outside to the local network, this results in an implicit "Deny All" strategy.

Note: If you operate a web server in your LAN, which has been permitted access to this service from the outside (see on page 579), stations from the Internet can establish connections to this server. The inverse masquerading has priority over the firewall in this case, as long as no explicit ‘Deny All’ rule has been set.

Setting up an explicit ‘Deny All’ Strategy

The ‘Deny All’ rule is by far the most important rule to help protect local networks. By this rule the firewall operates according to the principle: All actions that are not explicitly allowed remain forbidden. By means of this strategy, the administrator can be sure not to have forgotten an access method, because the means of access that exist are the ones that have been opened explicitly.

Hirschmann recommends that you set up the "Deny All" rule before connecting the LAN to the Internet via an OpenBAT device. In this way, you can analyze in the logging table (e.g. via LANmonitor) which connection attempts have been blocked by the firewall. With the help of this information, you can gradually extend the "Allow" rules of the firewall.

To increase protection and control of the data traffic, you should first guard against any data transfer by the firewall. Then, the necessary functions and communication paths are selectively allowed. This approach guards against so-called Trojan horses or e-mail viruses, which actively set up an outgoing connection on certain ports.

Typical examples of firewall settings include the following:

Rule Name	Source	Destination	Action	Service (target ports)
ALLOW_HTTP	Local network	All stations	transmit	http, https
ALLOW_FTP	Local network	All stations	transmit	ftp
ALLOW_EMAIL	Local network	All stations	transmit	MAIL, NEWS
ALLOW_DNS_FORWARDING	Local network	IP address of device (or local network)	transmit	DNS
DENY_ALL	All stations	reject	reject	ANY

- Sample configuration: ‘Basic Internet’

- For a network coupling you permit additionally the communication between the involved networks:

Rule Name	Source	Destination	Action	Service
ALLOW_LAN1_TO_LAN2	LAN1	LAN2	transmit	ANY
ALLOW_LAN2_TO_LAN1	LAN2	LAN1	transmit	ANY

- If you operate e.g. an own web server, you selectively allow access to the server:

Rule Name	Source	Destination	Action	Service (target ports)
ALLOW_WEBSERVER	ANY	Webserver	transmit	http, https

- For diagnostic purposes it is helpful to allow ICMP protocols (e.g. ping):

Rule Name	Source	Destination	Action	Service (target ports
ALLOW_PING	Local network	ANY	transmit	ICMP

These rules can now be refined as needed - e.g. by the indication of minimum and maximum bandwidths for the server access, or by a finer restriction on certain services, stations or remote sites.

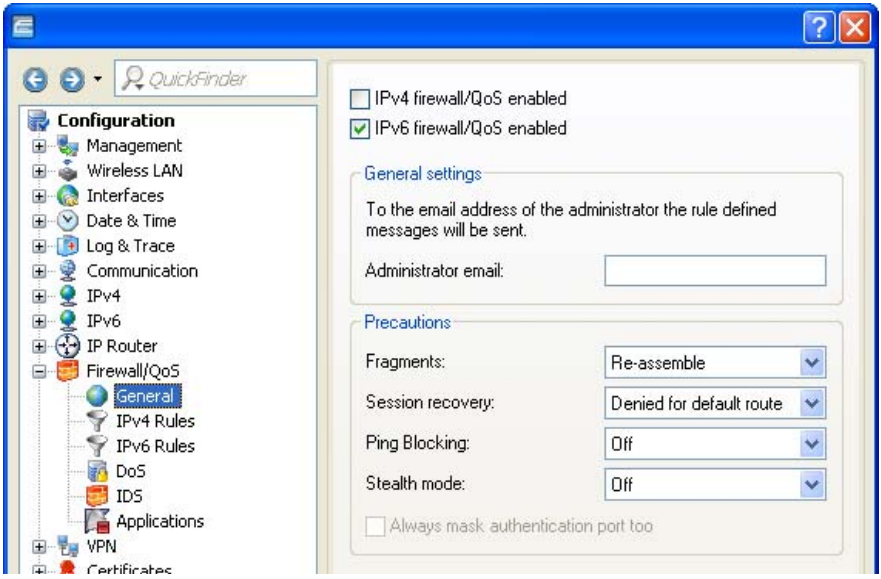
Note: The OpenBAT device automatically sorts firewall rules when creating the filter list. Thereby, the rules are sorted into the filter list on the basis of their level of detail. First, each specific rule is considered, then the general ones (e.g. Deny All). Examine the filter list in case of complex rule sets.

11.2 Firewall Configuration: LANconfig

The firewall can be configured using LANconfig, WEBconfig, and Telnet. The easiest way to configure the firewall is with LANconfig software.

11.2.1 General Firewall Parameters

Apart from individual firewall rules, the following general settings can be set for firewall. To access these general settings open the following dialog in the LANconfig software: `Configuration : Firewall/QoS : General`.



IPv4- bzw. IPv6 firewall/QoS enabled

This option switches on or off the entire firewall, including Quality of Service functions for IPv4 and/or IPv6.

Administrator e-mail

The firewall can trigger the alerting of a network administrator via e-mail. The 'administrator email' parameter contains the e-mail address to which the alerting mails are sent.

Fragments

Some attacks from the Internet try to outsmart the firewall by fragmenting packets into several small units. One of the main features of stateful inspections the ability to re-assemble fragments into entire packets, then check them against firewall rules. You can configure the firewall to treat fragmented packets as follows:

- Filter:
  The firewall discards packet fragments.
- Route:
  The firewall allows packet fragments to pass without further checking, provided the packet fragments are otherwise permitted by filter settings.
- Re-assemble:
  Fragmented packets are buffered and re-assembled into complete IP packets. The re-assembled packets are checked and treated according to filter settings.

Session recovery

The firewall adds the permitted connections into the connection list. Entries are automatically removed from the list after a timeout period, during which no data has been transmitted over this connection.

General TCP aging settings can close a connection before data packets requested by a remote station have been received. In this case it is possible for a connection entry that has been closed to continue to appear in the connection list.

Use this parameter to specify firewall behavior when it receives packets for a closed connection:

- Always allowed:
  The firewall re-establishes the connection if the packet belongs to a previously listed connection.
- Always denied:
  The firewall does not re-establish the session and discards the packet.
- Denied for WAN:
  The firewall re-establishes the session if the packet source was an interface other than a WAN interface.
- Denied for default route:
  The firewall re-establishes the session if the packet wasn't received from the default route (e.g. Internet).

Note: Because the virtual router takes action based on its analysis of the interface-tag, routes other than the untagged default route can be treated as the default route:

– When a packet is received at a WAN interface, then the WAN interface is considered by the firewall to be a default route if either a tagged or an untagged default route refers to this WAN interface.

– If a packet is received at a LAN interface and is to be routed to a WAN interface, then the WAN interface is considered to be a default route if either the untagged default route or a default route tagged with the interface tag refers to this WAN interface.

Default route filters are also effective if the default route is in the LAN. In this case, the filter takes effect when:

– A packet received over a tagged LAN interface is to be sent over a default route tagged with the interface, or

– A packet from another router was received at a tagged LAN interface and there is a default route with the interface tag to the packet's source address, or

– A packet was received from the WAN and is to be sent to the LAN via a default route with any tag.

Ping blocking

Hiding the router increases security. Many attacks start with a search for workstations or open ports by making harmless inquiries via the "ping" command or a port scan. Each response—even the answer "I'm not here"—indicates that the attacker has found a potential target. To help avoid these attacks, the OpenBAT device can be configured to suppress responses to these inquiries.

To achieve this, the OpenBAT device can be configured not to answer ICMP echo requests. At the same time TTL-exceeded messages of a trace route are also suppressed. The possible settings are:

- Off:
  ICMP responses are not blocked.
- Always:
  ICMP responses are always blocked.
- WAN only:
  ICMP responses are blocked on WAN connections.
- Default route only:
  ICMP responses are blocked on default route (usually Internet).

Stealth mode

The behavior of the OpenBAT device with respect to TCP and UDP connections can inform attackers of its existence. Depending on the surrounding network, it may make sense to silently reject TCP and UDP packets instead of answering with a TCP RESET or an ICMP message (port unreachable), if no listener for the respective port exists.

Note: If ports without listeners are hidden, this will create a challenge for masked connections. In this case, such a port can be separately configured.

Stealth mode settings include:

- Off:
  All ports are closed and TCP packets are answered with a TCP reset.
- Always:
  All ports are hidden and TCP packets are silently discarded.

- WAN only:
  On the WAN side all ports are hidden; on the LAN side all ports are closed.
- Default route only:
  Ports are hidden on the default route (usually Internet) and closed on all other routes.

Always mask authentication port too

Hiding TCP or UDP ports creates challenges for masked connections. If, for example, the so called 'Authenticate' or 'Ident' inquiries from special mail or news servers are returned to receive further user data and your device does not reject them, the corresponding connections will deliver a timeout. This can slow down mail or news delivery significantly.

To overcome this challenge, stealth mode is temporarily disabled for the specific port. The firewall recognizes that the internal stations intend to establish connections to a mail (SMTP, POP3, IMAP2) or news (NNTP) server, and opens the port for 20 seconds.

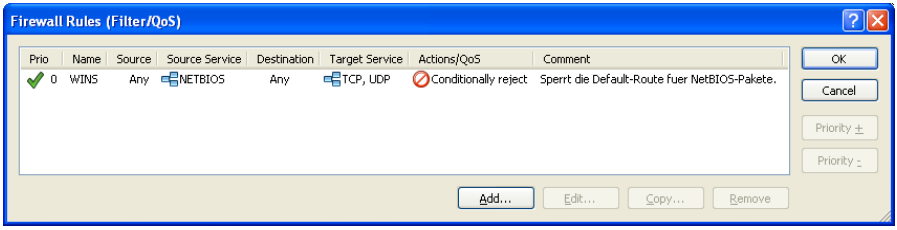
De-select this parameter to suppress the short-term cancellation of the stealth mode for the authentication port.

Note: Selecting this option significantly slows news and mail delivery.

11.2.2 Creating a New IPv4 Firewall Filter Rule

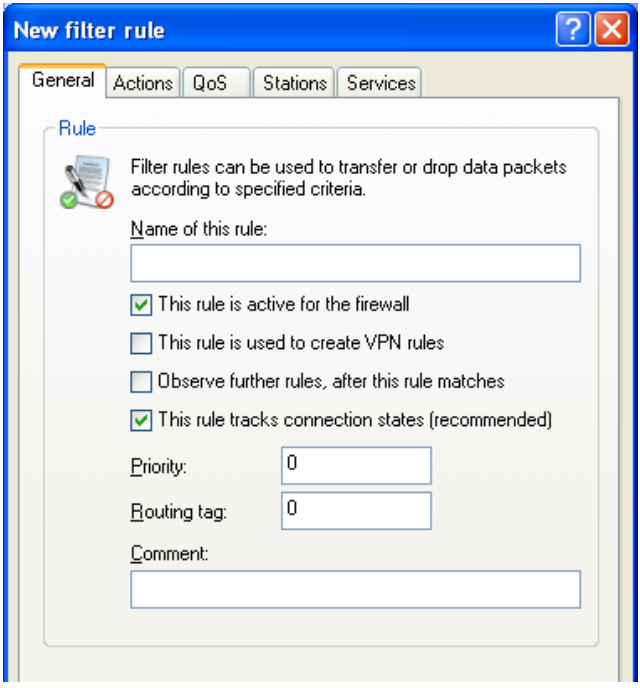
A new IPv4 firewall filter rule can be created in the ‘New filter rule’ dialog. To open this dialog:

☐ In the `Configuration : Firewall/QoS : IPv4 Rules` window, click "Rules" to open the rules list:



☐ In the ’Firewall Rules’ window (above,) click ’Add...’ to open the ‘New filter rule’ dialog (below).

☐ In the ’New filter rule’ dialog, click the ’General’ tab.



The settings in this dialog are described, below.

Activate the Rule

Activate the firewall rule by selecting the corresponding checkbox. If you uncheck this box, you can temporarily disable the rule without deleting it.

Use the Rule to Create VPN Rules

A VPN rule takes the details of the source and destination networks from the firewall rules, among others. By enabling this option, a VPN rule is derived from this firewall rule. For more information on this subject see the VPN chapter about creating rules (see on page 418 „Establishing VPN Network Relationships“).

Observe Further Rules

Some filters cannot be implemented using a single rule. For example, a company with three departments might want to limit bandwidth to each department to 512kbps, while at the same time limiting bandwidth to all three departments collectively to 1024 kbps. This can be accomplished by multi-level checking of multiple firewall rules. In this example:

– Step 1 checks to see if the data rate of the individual department exceeds the limit of 512 kbps.

– Step 2 checks to see if the data rates of all departments together exceed the overall limit of 1024 kbps.

If the ‘Observe further rules...’ option is not selected, a packet is checked until the first filter rule applies. The first time a filter applies, the firewall takes the appropriate action. The packet is not checked to see if additional rules apply to the packet.

But if the ‘Observe further rules...’ option is selected for the first rule applied to the packet, the firewall continues to apply other rules against the packet. This process continues until either:

– a rule applies to the packet, for which the ‘Observe further rules...’ option is not activated, or

– all remaining rules in the list have been applied to the packet.

- **Track Connection States**

  If selected, the firewall performs stateful inspections on data packets entering the firewall.

- **Priority**

  The OpenBAT device applies firewall rules according to a pre-defined priority. General rules (e.g. Deny All) are applied first, followed by special rules. It is possible to manually change the prioritization of rules. The higher the priority of the firewall rule—beginning with 1—the earlier it will be placed in the associated filter list. A value of 0 places no special priority on the rule.

  Note: For complex rule types, please refer to the description of the filter list (see on page 730).

- **Routing tag**

  The routing tag is used by the device to identify the ARF context from which a packet was received. Using this tag restricts the use of firewall rules to certain ARF contexts.

11.2.3 Firewall filter rule settings and actions

This section shows you how to configure the parameters that determine:

- Connection:
  To which stations and protocols does the filter rule apply?
- Conditions:
  Is the effectiveness of the rule limited by other conditions?
- Trigger:
  What threshold values trigger the rule?

- Action:
  How should the firewall handle data packets to which the rule applies when the threshold trigger is reached?
- Further measures:
  Should further measures be initiated in addition to the packet action?
- Quality of Service (QoS):
  Do certain data packets enjoy prioritized treatment by virtue of their QoS tags?

All of these settings and actions can be configured in dialogs in, or linked to, the ‘New filter rule’ dialog.

Note: The settings conditions, trigger, action and further measures together constitute a so-called ’action set’. Each firewall rule can contain a number of action sets. If the same trigger is used for several action sets, the sequence of action sets can be adjusted.

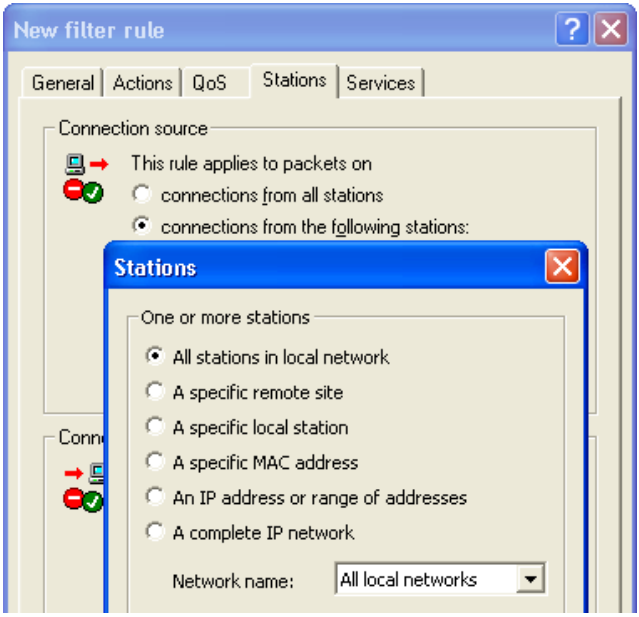
Connection

The connection element of a firewall rule defines the data packets to which the firewall filter rule applies. A connection is defined by its source and destination stations, and the services or protocols it requires.

To specify the source and destination stations for a rule:

☐ In the ‘New filter rule’ dialog, click the ‘Stations’ tab.

☐ If you select ‘connections from the following stations’, you can click ‘Add...’ to include less than all stations in the rule.



You can add the following connection source and destination station selections to the rule:

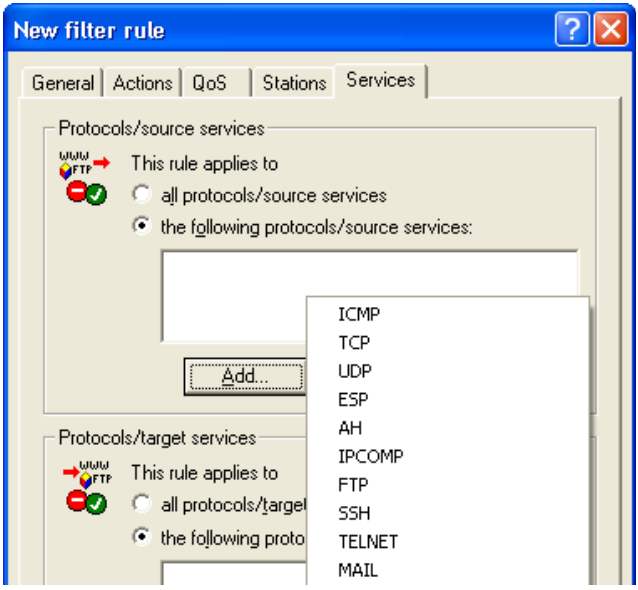
– all stations
– all stations in the LAN
– a specific remote site
– a specific local station
– a specific MAC address
– an IP address or range of addresses
– a complete IP network

You can operate with host names only if the OpenBAT device can transform their names into IP addresses. For that purpose the device needs to have learned the names via DHCP or NetBIOS, or you need to enter the assignment statically in the DNS or IP routing table. An entry in the IP routing table can therefore assign a name to a whole network.

Similarly, you can configure the rule to apply to all or some protocols and services. To do so:

☐ In the ‘New filter rule’ dialog, click the ‘Services’ tab.

☐ If you select ‘the following protocols/source services’ you can click ‘Add...’and apply less than all services or protocols to the rule.



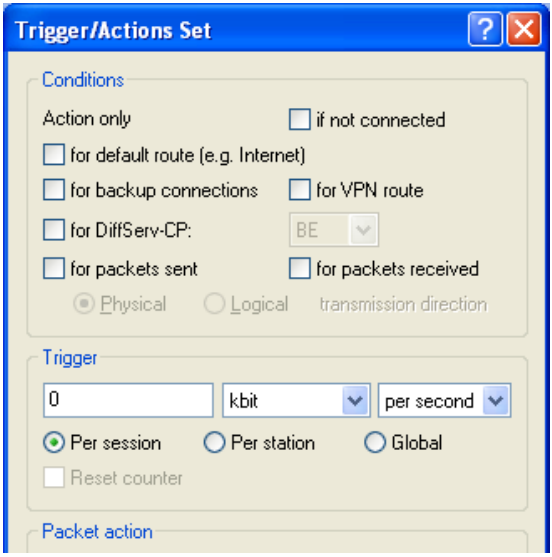
The service is determined by the combination of an IP protocol with respective source and/or destination port. For frequently used services (www, mail, etc.) the appropriate combinations are already predefined in the OpenBAT device.

Trigger

The trigger—or limit—describes a quantified threshold value that needs to be exceeded on the defined connection before the filter action is applied to a data packet. To set a trigger:

☐ In the ‘New filter rule’ dialog, click the ‘Actions’ tab.

☐ Click ‘Add...’ and select ‘Add custom action...’ to open the ‘Trigger/ Actions Set’ dialog.



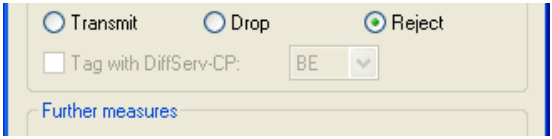
A trigger is set using the following parameters:

- Value: the measure of the trigger. This field accepts SI prefixes (k, Ki, M, Mi, G, Gi) as well as the SI unit bit, which divides the value by 8 when the entry field is exited.
- Unit: kbit, kByte, packets, sessions, %bandwidth
- Periodic reference: absolute, per hour, per minute, per second
- Scope: per session, per station, or global

If the rule applies, different counters are started. Either all packets or bytes that match this rule are counted globally or a specific counter will be started separately for every station (local host) or session (logical connection). The specific counter will either reset after the specified period of time (second, minute or hour) or it will count infinitely (absolute). An absolute counter can be reset if it exceeds its trigger value.

Packet Action

When a packet triggers a rule, the firewall acts in response. The specified action is also configured in the 'Trigger/Actions Set' dialog (just below the Trigger settings):



The firewall can take any of three packet actions:

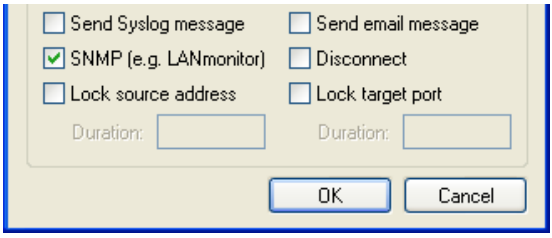
- Reject:
  The packet is not accepted; an ICMP reject notice is sent to the sender.
- Drop:
  The packet is silently rejected; no message is sent to the sender.
- Transmit:
  The packet is sent to its destination.

Note: A DiffServe codepoint (DSCP) tag can optionally be added to each transmitted packet. DSCP tags include:

– BE: Best Effort Normal packet (corresponds CS0)
– CS: 0 - 7 Class Selector Is compatible to the TOS field of the IPv4 header and corresponds to the precedence of unset TOS bits.
– AF: 0 - 4 / 0 - 3 Assured Forwarding The first digit represents the process priority and the second one represents the drop probability. The higher the priority and the lower the drop probability, the less frequently a packet will actually be dropped.
– EF: Expedited Forwarding Self declaring
– Value: An arbitrary tag—from 0 to 63—can be added.

Further Measures

In addition to discarding or accepting the filtered data packets, the firewall can also take additional measures when a data packet has been registered by the filter. These further measures are also configured in the 'Trigger/Actions Set' dialog (just below the 'Packet action settings'):



One or more of the following further measures can be set:

- Send Syslog message:
  Sends a message via the SYSLOG module to a SYSLOG client, that has been defined in the following page: `Configuration : Log & Trace : General : Syslog servers`.
- Send e-mail message:
  Sends an e-mail message to the designated administrator. To configure e-mail:
  – configure the administrator's e-mail address in the `Configuration : Firewall/QoS : General` dialog
  – properly set up the SMTP e-mail account in the `Configuration : Log & Trace : SMTP Account` dialog
- SNMP (e.g. LANmonitor):
  Sends an SNMP trap that will be analyzed, e.g., by LANmonitor.

  Note: A message sent by any of the above three methods causes an entry to be made in the firewall event table.

- Disconnect:
  Cuts both the physical and logical connections over which the filtered packet has been received.

- Lock source address:
  Temporarily blocks packets that are received from a specific address.
- Lock target port:
  Temporarily blocks packets that are transmitted over a specific port.

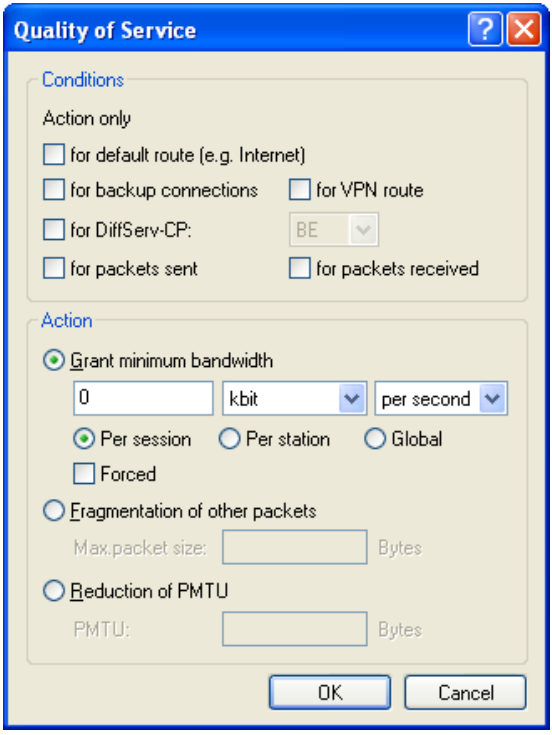
  Note: The duration of the source host or target port lock should be specified. Otherwise the respective addresses or ports will be permanently locked. These locks can be released on the device exclusively by using a Telnet console or WEBconfig.

QoS

You can also configure Quality of Service (QoS) settings for the rule, which assigns a relative priority to the handling of the packet. To access the QoS firewall rule configuration dialog:

☐ In the ‘New filter rule’ dialog, click the ‘QoS’ tab.

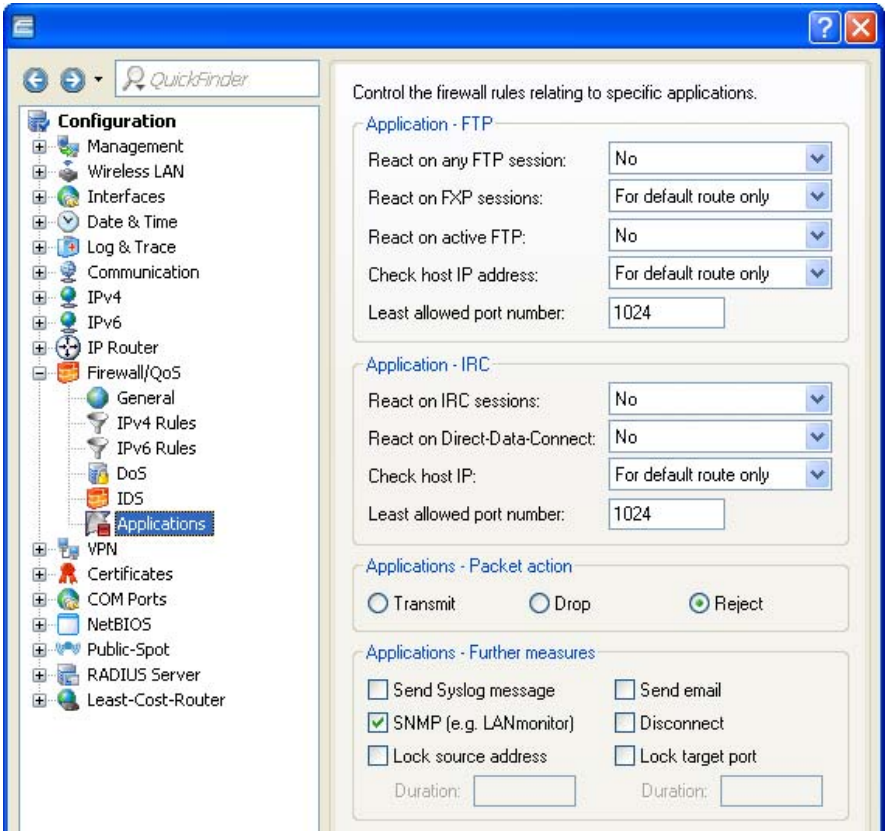
☐ Click ‘Add...’ and select ‘Add custom QoS...’ to open the ‘Quality of Service’ dialog.


Quality of Service
Conditions
Action only
for default route (e.g. Internet)
for backup connections
for VPN route
for DiffServ-CP:
BE
for packets sent
for packets received
Action
Grant minimum bandwidth
0
kbit
per second
Per session
Per station
Global
Forced
Fragmentation of other packets
Max.packet size:
Bytes
Reduction of PMTU
PMTU:
Bytes
OK
Cancel

11.2.4 Applying firewall rules to FTP and IRC connections

Special firewall rules can be configured and applied to file transfer protocol (ftp) and internet relay chat (IRC) connections, because of the unique threats presented by these two means of access to the local area network. To access the configuration dialog for these settings:

☐ Open the `Configuration : Firewall/Qos : Applications` dialog:



Use the settings described below to configure special handling for packets sent to the firewall over ftp and IRC connections:

- ftp applications:
  If an ftp session is recognized on any port, the countermeasures specified below apply:
  - React on Any FTP session: Indicate if, and over which routes, an ftp transmission should receive special handling. Default setting is 'Off'.
  - React on FXP sessions: Indicate if, and on which routes, a Site-To-Site transfer—via the file exchange protocol (FXP)—should receive special handling. Default setting is 'For default route only'.
  - React on active FTP: Indicate if, and on which routes, an ftp transmission in active mode should receive special handling. Default setting is 'Off'.
  - Check host IP address: Indicate if, and on which routes, the address transferred in the ftp command channel should be checked against the source address of the ftp client. If it does not match, the firewall performs packet action specified below.
  - Least allowed port number: The lower boundary for active ftp. Default setting is port '1024'.
- IRC applications:
  If an IRC session is recognized on any port, the countermeasures specified beneath apply:
  - React on IRC sessions: Indicate if, and over which routes, an IRC transmission should receive special handling. Default setting is 'Off'.
  - React on Direct-Data-Connect: Indicate if, and on which routes, Direct-Data-Connect (DDC - private chats and file transfers) should receive special handling. Default setting is 'Off'.
  - Check host IP address: Indicate if, and on which routes, the address transferred in the DDC command channel should be checked against the source address of the IRC client. If it does not match, the firewall performs packet action specified below. This check is skipped if a Site-To-Site transfer takes place and is already allowed. Default setting is 'For default route only'.
  - Least allowed port number: The lower boundary for active DDC. Default setting is port '1024'.

- Packet action:
  Indicate the action the firewall should take with respect to packets that are responsible for triggering an action or exceeding a limit:
  - Transmit: the packet is forwarded according to its address.
  - Drop: no notice to the addressor is sent.
  - Reject: an ICMP reject notice is sent to the packet source.
- Further measures:
  One or more of the following further measures can be set:
  - Send Syslog message: Sends a message via the SYSLOG module to a SYSLOG client, that has been defined in the following page:
    `Configuration : Log & Trace : General : Syslog servers`
  - Send e-mail message: Sends an e-mail message to the designated administrator. Both the administrator's e-mail address and the SMTP e-mail account need to be properly configured.
  - SNMP (e.g. LANmonitor): Sends a SNMP trap, that will be analyzed e.g. by LANmonitor.
  - Disconnect: Cuts both the physical and logical connections over which the filtered packet has been received.
  - Lock source address: Temporarily blocks packets that are received from a specific address.
  - Lock target port: Temporarily blocks packets that are transmitted over a specific port.

  Note: The duration of the source host or target port lock should be specified. Otherwise the respective addresses or ports will be permanently locked. These locks can be released on the device exclusively by using a Telnet console or WEBconfig.

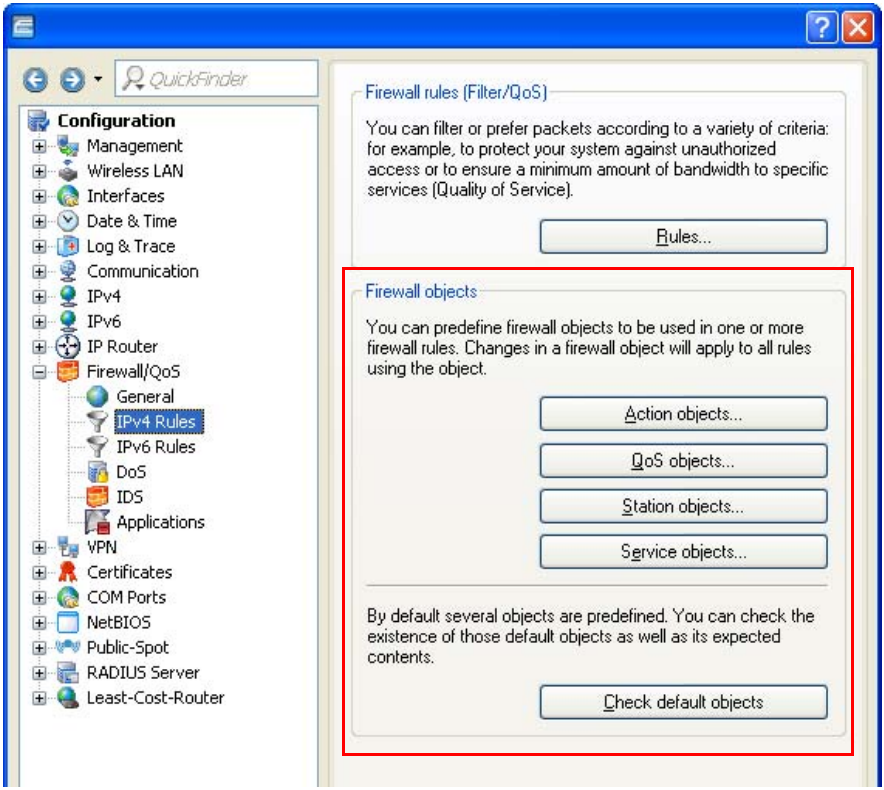
11.2.5 Defining Firewall Objects

When configuring the firewall with LANconfig, various objects can be defined that are used in the firewall rules. This means that frequently used definitions (such as a particular action) do not need to be re-entered for every rule. Instead they can be stored once at a central location.

Note:

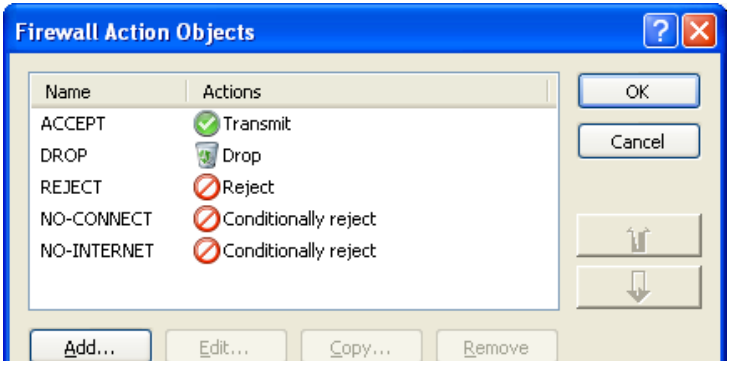
- Be aware that a change to a firewall object affects all of the firewall rules that use this object. For this reason, all firewall rules that also use these objects are displayed when you make changes to firewall objects.
- Existing firewalls (in the % notation) are not automatically converted to the object-orientated form when the configuration is opened in LANconfig. The KnowledgeBase contains the pre-defined firewall settings used by the new objects.

New firewall objects can be defined in LANconfig at the following dialog:
`Configuration : Firewall/QoS : IPv4 Rules`.


QuickFinder
Configuration
Management
Wireless LAN
Interfaces
Date & Time
Log & Trace
Communication
IPv4
IPv6
IP Router
Firewall/QoS
General
IPv4 Rules
IPv6 Rules
DoS
IDS
Applications
VPN
Certificates
COM Ports
NetBIOS
Public-Spot
RADIUS Server
Least-Cost-Router
Firewall rules (Filter/QoS)
You can filter or prefer packets according to a variety of criteria: for example, to protect your system against unauthorized access or to ensure a minimum amount of bandwidth to specific services (Quality of Service).
Rules...
Firewall objects
You can predefine firewall objects to be used in one or more firewall rules. Changes in a firewall object will apply to all rules using the object.
Action objects...
QoS objects...
Station objects...
Service objects...
By default several objects are predefined. You can check the existence of those default objects as well as its expected contents.
Check default objects

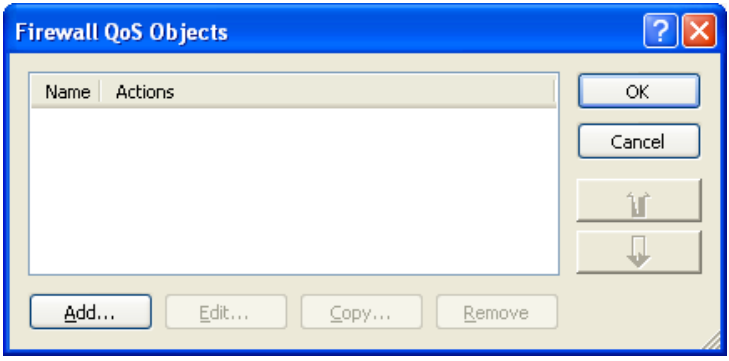
Action Objects

Use the ‘Firewall Action objects’ configuration dialogs to create firewall actions, each of which is a unique collection of condition, limit trigger, packet action and other measures to be used by the firewall rules.



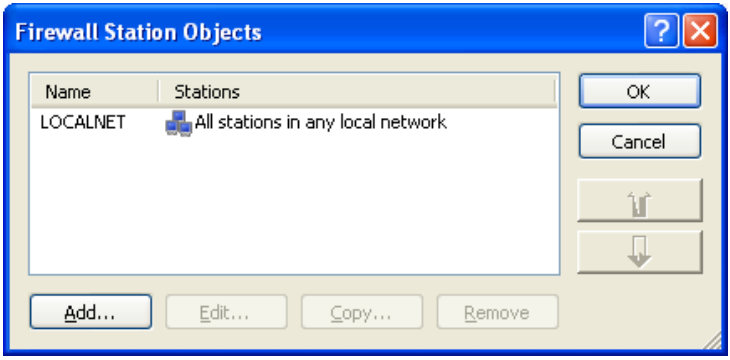
QoS Objects

Use the ‘Firewall QoS objects’ configuration dialog to set the minimum bandwidths that the firewall rules allocate to data packets.



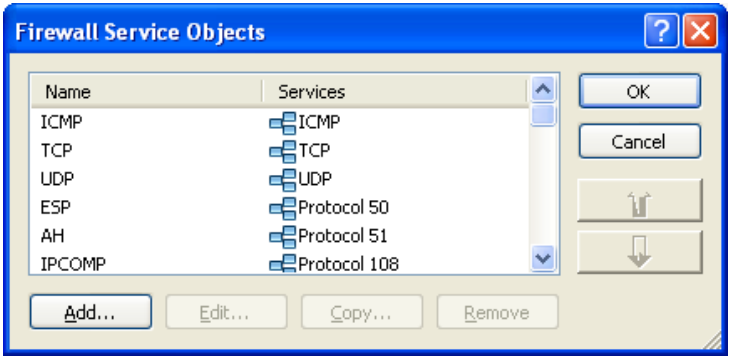
Station Objects

Use the ‘Firewall Station Objects’ configuration dialogs to define stations that the firewall rules can use as packet source or destination. The station objects are not restricted to any particular source or destination, but can be used as required by the firewall rules. In the context of Advanced Routing and Forwarding (ARF) you can specify a certain IP network as station object:



Service Objects

The IP protocols and the source/destination ports to be used by the firewall rules are defined here.



11.3 Configuring the IPv4 Firewall: WEBconfig and Telnet

11.3.1 Rules Table

The Rules table links various pieces of information of a firewall rule. The rule contains the protocol to be filtered, the source, the destination and the firewall action to be executed. For every firewall rule there is also an on/off switch, a priority, the option to link with other rules.

Just as with LANconfig, WEBconfig can be used to configure the firewall with the help of objects. The % notation described as follows is necessary for defining objects or actions.

To access the IPv4 rules table, follow these steps:

`Configuration : Firewall/QoS :IPv4 rules: Rule table`

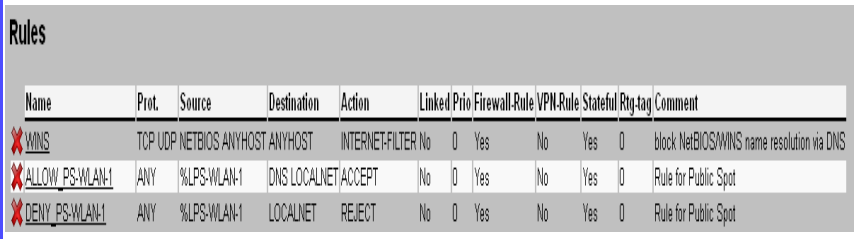


Figure 123:IPv4 Firewall Rules Table in WEBconfig

Note: Existing firewalls in the % notation are not automatically converted to the object-orientated form. However, the KnowledgeBase contains the pre-defined firewall settings used by the new objects.

The operating system of the OpenBAT device uses a special syntax for the firewall rules. This syntax enables the representation of complex interrelationships for the testing and handling of data packets in the firewall with just a few characters. The rules are defined in the rules table. Pre-defined objects can be stored in two further tables so that frequently used objects do not have to be entered into the operating system syntax every time:

- Firewall actions are stored in the Action table.
- Stations and service references are stored in the Object table.

Note: You can use the objects from in these tables to define rules, although this is not compulsory. These tables are designed to simplify the use of frequently used objects.

The definition of firewall rules can contain entries in the object table for protocols, services, stations and the action table for firewall actions, and also direct definitions in the appropriate operating system syntax (e.g. %P6 for TCP).

Note: For direct input of level parameters in the operating system syntax, the same rules apply as specified in the following sections for protocols, source/ destination and firewall actions.

11.3.2 Objects Table

Elements/objects that are to be used in the firewall rules table are defined in the Objects table.
To access the IPv4 objects table, follow these steps:

```
Configuration : Firewall/QoS :IPv4 rules: Object table
```

Objects

Name	Description
ANYHOST	%A0.0.0.0 %M0.0.0.0
LOCALNET	%L
ANY	
ICMP	%P1
TCP	%P6
UDP	%P17
ESP	%P50
AH	%P51
IPCOMP	%P108
FTP	TCP %S21
MAIL	TCP %S25,110,143
SECURE-MAIL	TCP %S993,995
HTTP	TCP %S80
HTTPS	TCP %S443
WEB	TCP %S80,443
NEWS	TCP %S119
TFTP	UDP %S69
IPSEC	UDP %S500,4500
SSH	TCP %S22
TELNET	TCP %S23
DNS	TCP UDP %S53
NETBIOS	TCP UDP %S137-139

Figure 124:IPv4 Firewall Objects Table in WEBconfig

Objects can be:

- Individual computers (MAC or IP address, hostname)
- Complete networks
- Protocols
- Services (ports or port areas, e.g. http, Mail&News, ftp, ...)

These elements can be combined and hierarchically structured in any way. For example, objects for the TCP and UDP protocols can be defined first. Building upon this, objects can subsequently be created, for example, for ftp (= TCP + ports 20 and 21), http (= TCP + port 80) and DNS (= TCP, UDP + port 53). These can in turn be combined into one object that contains the definitions of every individual object.

11.3.3 Action Table

A firewall action comprises of a condition, a limit, a packet action and other measures. As with the elements of the object table, firewall actions can be given a name and be combined with each other in any way recursively. The maximum recursion depth is limited to 16. They can also be entered into the actions field of the rules table directly.

To access the IPv4 actions table, follow these steps:

```
Configuration : Firewall/QoS :IPv4 rules: Action table
```

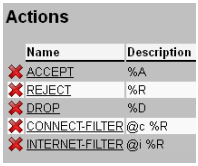


Figure 125:Firewall Action Table in WEBconfig

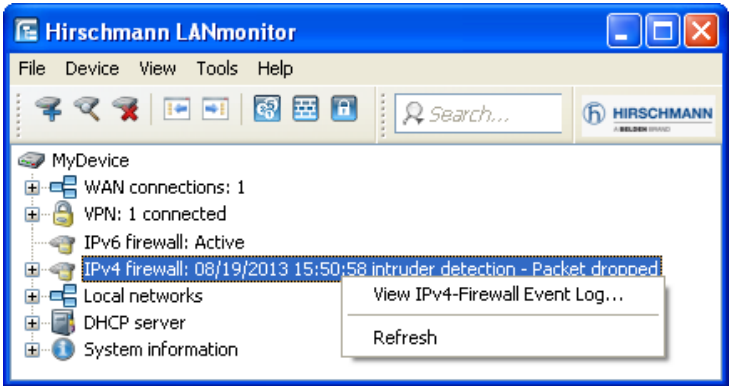
11.4 Firewall Diagnosis

All events, conditions and connections of the firewall can be logged and monitored in detail using either LANmonitor software or WEBconfig. The examples in this section are presented using LANmonitor software. However, all dialog and lists presented here can also be accessed at the following location:

`HiLCOS Menu Tree : Status : IP Router`

11.4.1 The Firewall Log Table

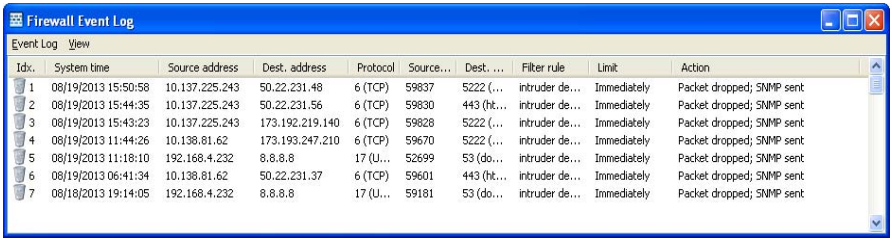
The easiest way to inspect firewall performance is by opening the ‘Log table’ from LANmonitor.



To open the log table in LANmonitor:

☐ Select the firewall and click on the right mouse button.

☐ In the pop-up menu, select ‘Firewall Event Log’:


Firewall Event Log
Event Log View
Idx. System time Source address Dest. address Protocol Source... Dest. ... Filter rule Limit Action
1 08/19/2013 15:50:58 10.137.225.243 50.22.231.48 6 (TCP) 59837 5222 (... intruder de... Immediately Packet dropped; SNMP sent
2 08/19/2013 15:44:35 10.137.225.243 50.22.231.56 6 (TCP) 59830 443 (ht... intruder de... Immediately Packet dropped; SNMP sent
3 08/19/2013 15:43:23 10.137.225.243 173.192.219.140 6 (TCP) 59828 5222 (... intruder de... Immediately Packet dropped; SNMP sent
4 08/19/2013 11:44:26 10.138.81.62 173.193.247.210 6 (TCP) 59670 5222 (... intruder de... Immediately Packet dropped; SNMP sent
5 08/19/2013 11:18:10 192.168.4.232 8.8.8.8 17 (U... 52699 53 (do... intruder de... Immediately Packet dropped; SNMP sent
6 08/19/2013 06:41:34 10.138.81.62 50.22.231.37 6 (TCP) 59601 443 (ht... intruder de... Immediately Packet dropped; SNMP sent
7 08/18/2013 19:14:05 192.168.4.232 8.8.8.8 17 (U... 59181 53 (do... intruder de... Immediately Packet dropped; SNMP sent

The table contains the following fields:

Element	Description
Idx	Current index (so that the table can be polled also via SNMP)
Timestamp	System time in UTC codification (will be transformed on displaying of the table into clear text)
Src address	Source address of the filtered packet
Dst address	Destination address of the filtered packet
Protocol	Protocol (TCP, UDP etc.) of the filtered packet
Src port	Source port of the filtered packet (exclusively with port-related protocols)
Dst port	Destination port of the filtered packet (exclusively with port-related protocols)
Firewall rule	Name of the rule, which has raised the entry
Limit	Bit field, which describes the crossed limit, which has filtered the packet. There following values are currently defined: 0x01 Absolute amount, 0x02 Number per second 0x04 Number per minute 0x08 Number per hour: 0X10 Global limit 0x20 Byte limit (if not set, it is a packet limit) 0x40 Limit only applies in the inbound direction 0x80 Limit only applies in the outbound direction
Action	Bit field which lists all the actions performed. Currently, the following values are defined: 0x00000001 Accept 0x00000100 Reject 0x00000200 Dial-up filter 0x00000400 Internet (Default Route) filter 0x00000800 Drop 0x00001000 Disconnect 0x00004000 Lock source address 0x00020000 Lock destination address and port 0x20000000 Send SYSLOG notification message 0x40000000 Send SNMP trap 0x80000000 Send e-mail

Note: All Firewall actions are likewise displayed by the IP router trace function, and some OpenBAT devices have a Firewall LED that signals each filtered packet.

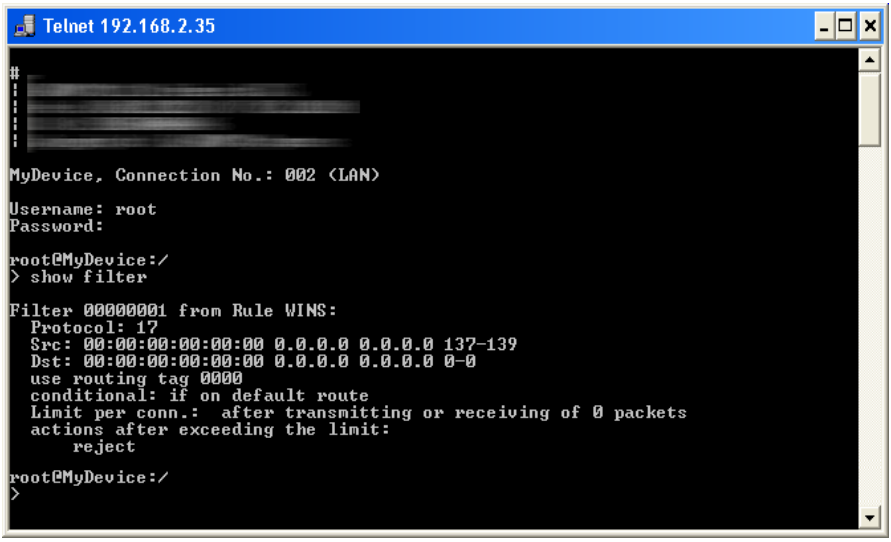
11.4.2 The Filter List

The filter list displays filters generated by rules defined in the action, object and rules tables.

Note: Manually entered filter rules do not indicate potential anomalies or generate exception response messages. If you configure filters manually, you should examine each entry in the filter list on a case by case basis to determine whether that filter is performing as intended.

You can view the contents of the filter list using Telnet by issuing the following command:

```
show filter
```



The firewall table contains the following fields

Element	Description
Idx	Current index (so that the table can be polled also via SNMP)
Prot	Protocol to be filtered, e.g. 6 for TCP or 17 for UDP
Src MAC	Ethernet source address of the packet to be filtered or 000000000000, if the filter should apply to all packets
Src address	Source IP address or 0.0.0.0, if the filter should apply to all packets
Source mask	Source network mask, which determinates the source network together with the source IP address, or 0.0.0.0, if the filter should apply to packets from all networks
S start	Start source port of the packets to be filtered.
S end	End source port of the packets to be filtered. Makes up the port range together with the start source port, in which the filter takes effect. If start and end port are 0, then the filter is valid for all source ports.
Dst-MAC	Ethernet destination address of the packet to be filtered or 000000000000, if the filter should apply to all packets.
Dst address	Destination address or 0.0.0.0, if the filter should apply to all packets.
Dst mask	Destination network mask, which determinates the destination network together with the destination IP address, or 0.0.0.0, if the filter should apply to packets to all networks.
D start	Start destination port of the packets to be filtered.
end	End destination port of the packets to be filtered. Makes up the port range together with the start destination port, in which the filter takes effect. If start and end port are 0, then the filter is valid for all destination ports.

Element	Description
Action	Into this column, the main action is unveiled as a text, which will be executed when the first limit has been exceeded. The first limit can be also an implicit limit, e.g. if exclusively one limit for the restriction of the throughput was configured. Then an implicit limit - linked with an accept action - is inserted. In this case, accept is unveiled as main action. You can see the complete actions under the command show filter.
Linked	Specifies if this rule is a “first match rule” (linked = no). The device appraises further rules only if a linked rule matches.
Prio	Priority of the rule having generated the entry.
Rtg tag	Routing tag including the data packets which are captured by this entry

11.4.3 The Connection List

The connection table files source address, destination address, protocol, source port, destination port, etc. of a connection, as well as possible actions. This table is sorted according to source address, destination address, protocol, source port and destination port of the packet, which caused the entry in the table.

The connection list contains these fields:

Element	Description
Src address	Source address of the connection
Dst address	Destination address of the connection
Protocol	Used protocol (TCP/UDP etc.) The device refers to the protocol with its decimal value.
Src port	Source port of the connection. The port is exclusively indicated with port-related protocols (TCP/UDP) or protocols, which own a comparable field (ICMP/GRE)
Dst port	Destination port of the connection (with UDP connections, this one is occupied exclusively with the first answer)
Rtg tag	Routing tag of the connection
Timeout	Each entry ages out with the time of this table, thus the table does not overflow with died connections.
Flags	Flags save the state of a connection and further (internal) information into a bitfield. The following values are possible for a state: new, establish, open, closing, closed, rejected (according to the TCP flags: SYN, SYN ACK, ACK, FIN, FIN ACK and RST).UDP connections know the conditions new, open and closing (the last one exclusively, if the UDP connection is linked with a condition-afflicted control path. This is e.g. the case with protocol H.323.)

Element	Description
Filter rule	Name of the rule, which has generated the entry (determines also the actions to be executed), when a suitable packet is received.
Src route	Name of the remote station, over which the first packet has been received.
Dst route	Name of the remote station, where the first packet will be sent to.

Flags of the connection list include:

Element	Description
00000001	TCP: SYN sent
00000002	TCP: SYN/ACK received
00000004	TCP: waiting for ACK of the server
00000008	All: Connection opened
00000010	TCP: FIN received
00000020	TCP: FIN sent
00000040	TCP: RST sent or received
00000080	TCP: session will be re-established
00000100	ftp: passive ftp connection will be established
00000400	H.323: belonging to T.120 connection
00000800	connection via loopback interface
00001000	checking concatenated rules
00002000	rule is catenated
00010000	destination is on local route
00020000	destination is on default route
00040000	destination is on VPN route
00080000	physical connection is not established
00100000	source is on default route
00200000	source is on VPN route
00800000	no route for destination
01000000	contains global actions with condition

11.4.4 Port Block List

Address, protocol and port of a destination station are filed in the port block list, if blocking of the destination port on the destination station was selected as a filter's packet action. This table is likewise a sorted semi-dynamic table. Sorting is done according to address, protocol and port. The table contains the following elements:

Element	Description
Address	Address of the station, to which the blocking should apply.
Protocol	Used protocol (TCP/UDP etc.). The device refers to the protocol with its decimal value.
Port	Port to close at the station. If the respective protocol is not port related, then the entire protocol for this station becomes closed.
Timeout	Duration of the blocking in minutes.
Filter rule	Name of the rule, which has generated the entry (determines also the actions to be executed), when a suitable packet is received.

11.4.5 Host Block List

The address of a station is filed in the host block list, if blocking of the sender was selected in a filter's packet action. This table is a sender address sorted semi-dynamic table and contains the following elements:

Element	Description
Address	Address of the station, to which the blocking should apply.
Timeout	Duration of the blocking in minutes.
Filter rule	Name of the rule, which has generated the entry (determines also the actions to be executed), when a suitable packet is received.

11.5 Firewall Limitations

In addition to understanding how the firewall works, be aware of its limitations, and how to supplement the firewall if necessary. The firewall does not guard against malicious content entering the network through a permitted path. Although a firewall may stop some viruses and worms from entering the network, that is because the packets containing them were blocked from entering a port. However, no firewall alone provides comprehensive security against viruses.

A firewall does not hinder lurkers, who wish to read unencrypted communications sent beyond the firewall.

11.6 Combating intrusion attempts Intrusion detection

A firewall examines data traffic that attempts to pass between networks, and rejects those packets that lack permission to access the network. In addition to attempts to access directly a computer in the protected network, intruders also mount attacks against the firewall itself, or attempt to outwit a firewall with falsified data packets.

The Intrusion Detection System (IDS) is designed to recognize, repel and keep a record of these attacks. When an intruding packet is detected, the IDS can provide notice of the event, via e-mail notification, SNMP traps or SYSLOG alarms. IDS checks the certain properties of the data traffic looking for conspicuous patterns, which indicate an attempted attack upon the network.

11.6.1 Examples of Break-in Attempts

- **Spoofing**

  In a spoofing attack, the sender of a packet poses as a different computer. This approach is taken either to trick the firewall, which trusts packets from the own network more than packets from untrusted networks, or to hide the source of an attack.

  The firewall guards itself against spoofing by route examination—it determines whether a packet is permitted over the specific interface over which it was received.

- **Port Scan Detection**

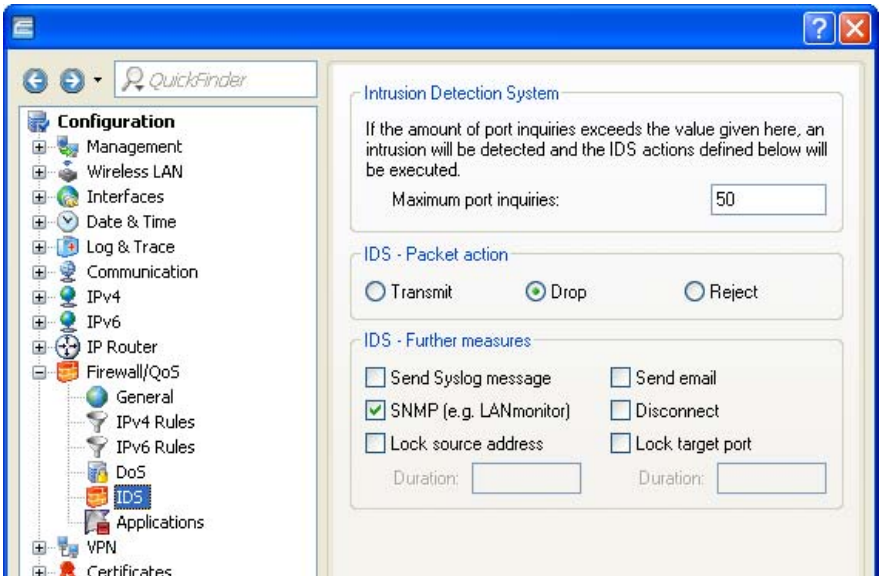
  The IDS attempts to detect port scans as they occur, then to report and react appropriately to this form of attack. The response is similar to the recognition of a 'SYN Flooding' attack: Any 'half-open' connections are also checked (the product of a TCP RESET sent by the scanned computer that lease a connection 'half-open').

  If a certain number of half-open connections between the scanned and the scanning computer exist, then this is reported as a port scan. In addition, the receipt of empty UDP packets is interpreted as an attempted port scan.

11.6.2 Configuring the IDS

To configure the firewall for intrusion detection:

☐ Open the `Configuration : Firewall/Qos : IDS` dialog:



The following parameters can be configured for the IDS:

- IDS: Use this section of the dialog to define an intrusion:
  - Maximum port inquiries: A number of intrusion attempts above this number trigger IDS responsive action.
- Packet action: Indicate the action the firewall should take with respect to an IDS attack:
  - Transmit: the packet is forwarded according to its address.
  - Drop: no notice to the addressor is sent.
  - Reject: an ICMP reject notice is sent to the packet source.
- Further measures:
  One or more of the following further measures can be set:
  - Send Syslog message: Sends a message via the SYSLOG module to a SYSLOG client, that has been defined in the following page:
    `Configuration : Log & Trace : General : Syslog servers`
  - Send e-mail message: Sends an e-mail message to the designated administrator. Both the administrator's e-mail address and the SMTP e-mail account need to be properly configured.
  - SNMP (e.g. LANmonitor): Sends a SNMP trap, that will be analyzed e.g. by LANmonitor.
  - Disconnect: Cuts both the physical and logical connections over which the filtered packet has been received.
  - Lock source address: Temporarily blocks packets that are received from a specific address.
  - Lock target port: Temporarily blocks packets that are transmitted over a specific port.

  Note: The duration of the source host or target port lock should be specified. Otherwise the respective addresses or ports will be permanently locked. These locks can be released on the device exclusively by using a Telnet console or WEBconfig.

11.7 Protection from denial of service attacks

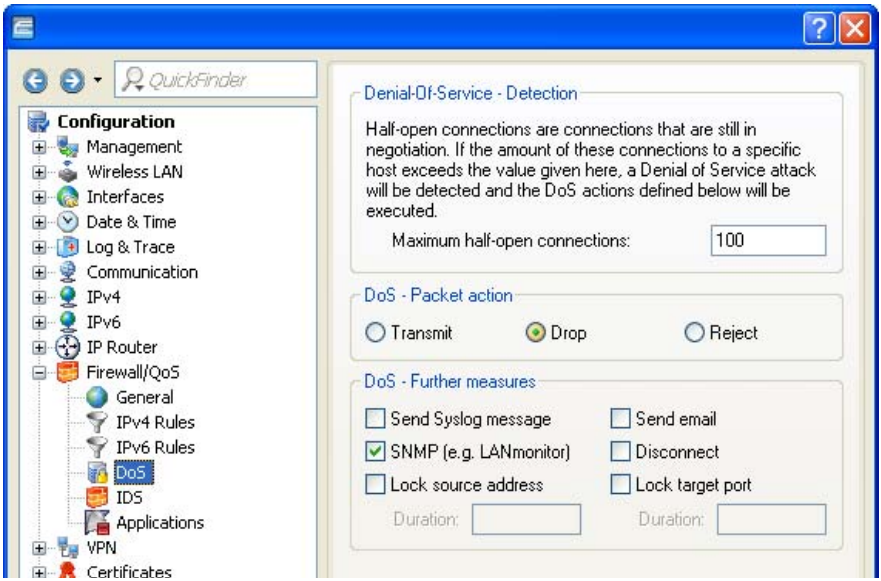
Some external attacks aim to block access to, and the functioning of, LAN services. Each OpenBAT device includes mechanisms that are designed to recognize well-known hacker attacks and continue to provide functionality in the face of such attacks.

11.7.1 Configuring DoS Blocking

In order to drastically reduce the susceptibility of the network to denial of service (DoS) attacks, packets from distant networks may be accepted exclusively if a connection has been initiated from the internal network, or the incoming packets have been accepted by an explicit filter entry (source: distant network, destination: local area network). The firewall tracks the connection state, source addresses and correctness of fragments for all explicitly permitted connections. This is performed with respect to both incoming and outgoing packets, since an attack could also be initiated from within the local area network. Address examination (against IP spoofing) and blocking of broadcasts into the LAN are continuously performed.

To configure the firewall to respond to denial of service attacks:

☐ Open the `Configuration : Firewall/Qos : DoS` dialog:



The following parameters can be configured for the IDS:

- DoS: Use this section of the dialog to define a DoS attack:
  - Maximum half-open connections: A number of half-open connections that triggers a responsive action.
- Packet action: Indicate the action the firewall should take with respect to an DoS attack:
  - Transmit: the packet is forwarded according to its address.
  - Drop: no notice to the addressor is sent.
  - Reject: an ICMP reject notice is sent to the packet source.
- Further measures:
  One or more of the following further measures can be set:
  - Send Syslog message: Sends a message via the SYSLOG module to a SYSLOG client, that has been defined in the following page:
    `Configuration : Log & Trace : General : Syslog servers`
  - Send e-mail message: Sends an e-mail message to the designated administrator. Both the administrator's e-mail address and the SMTP e-mail account need to be properly configured.
  - SNMP (e.g. LANmonitor): Sends a SNMP trap, that will be analyzed e.g. by LANmonitor.
  - Disconnect: Cuts both the physical and logical connections over which the filtered packet has been received.
  - Lock source address: Temporarily blocks packets that are received from a specific address.
  - Lock target port: Temporarily blocks packets that are transmitted over a specific port.

  Note: The duration of the source host or target port lock should be specified. Otherwise the respective addresses or ports will be permanently locked. These locks can be released on the device exclusively by using a Telnet console or WEBconfig.

12 IPv6

12.1 IPv6 basics

IPv4 (Internet Protocol version 4) is a protocol for unique addressing of nodes in a network and, at the time of writing, it has defined all of the IP addresses assigned globally. The limited availability of address space required the development of IPv6 (Internet Protocol version 6), which is to replace the former standard. With a different IP-address structure, IPv6 provides for a greater range of IP addresses and thus increases the possible number of participants in networks worldwide.

12.1.1 Why Use IPv6-standard IP Addresses?

The new IPv6 standard was developed for the following reasons:

- IPv4 address space allows for approximately four billion IP addresses for unique identities in networks. When the IPv4 standard was implemented in the '80s this address space was considered to be sufficient. Due to the enormous growth of the World Wide Web and the unexpectedly large number of computers and network devices, an address shortage has arisen that the IPv6 standard is intended to bridge.
- The increase in address space with IPv6 hampers the scanning of IP addresses by viruses and Trojans. The broader spectrum provides greater protection against attacks.
- IPv6 has been implemented with a view to the security requirements. For this reason it uses the security protocol IPSec (IP Security). This provides secure network communications on layer 3 whereas many of IPv4 security mechanisms only operate on higher layers.
- Simplified, fixed descriptors for data packets save on router processing power and thus accelerate the available throughput.

- IPv6 allows for easier and faster transmission of data in real time, making it suitable for multimedia applications such as Internet telephony and Internet TV.
- So-called mobile IPs allow you to use a fixed IP address to login to different networks. This allows you to log on with your laptop using the same IP address, whether you are in your home network, in a café or at work.

12.1.2 IP Address Structure According to the IPv6 Standard

The new IPv6 addresses are 128 bits long and the range of possible addresses can cater for about 340 sextillion network participants. IPv6 addresses consist of eight blocks of 16 bits and are written as hexadecimal numbers. The following is an example of a possible IPv6 address:

2001:0db8:0000:0000:0000:54f3:dd6b:0001/64

To improve the legibility of these IP addresses, zeros at the beginning of a block of numbers are omitted. It is also possible to omit one group of blocks that consist entirely of zeros. For the above example, one possible representation would be as follows:

2001:db8::54f3:dd6b:1/64

An IPv6 address consists of two components: A prefix and an interface identifier. The prefix denotes the membership of the IP address to a network, while the interface identifier (e.g. in the case of auto-configuration) is generated from a link-layer address, and thus belongs to a particular network card. The device can also generate interface identifiers from random numbers. This improves security. In this way, multiple IPv6 addresses can be assigned to a single component.

The prefix describes the first part of the IP address. The length of the prefix is ??shown as a decimal number after a slash. For the example given here the prefix is:

2001:db8::/64

The remainder of the IP address is the interface identifier. In our example, this is:

::54f3:ddb6:1

Compared with the IP addresses for the IPv4 standard, a number of changes have resulted in the structure of the new IPv6 addresses:

- While IPv4 addresses cater for an address space of 32 bits, the new length of 128 bits results in a significantly larger address space with IPv6. IPv6 addresses are four times longer than IPv4 addresses.
- An interface can have multiple IPv6 addresses due to the potential assignment of multiple prefixes to a single interface identifier. With the IPv4 standard, an interface has only one IP address.
- The automatic assignment of IPv4 addresses is always handled by a DHCP server. However, IPv6 can operate an auto-configuration, which makes the use of a DHCP server unnecessary. However, it is still possible to employ a DHCP server or to configure the IP addresses statically.

12.1.3 Stages of Migration

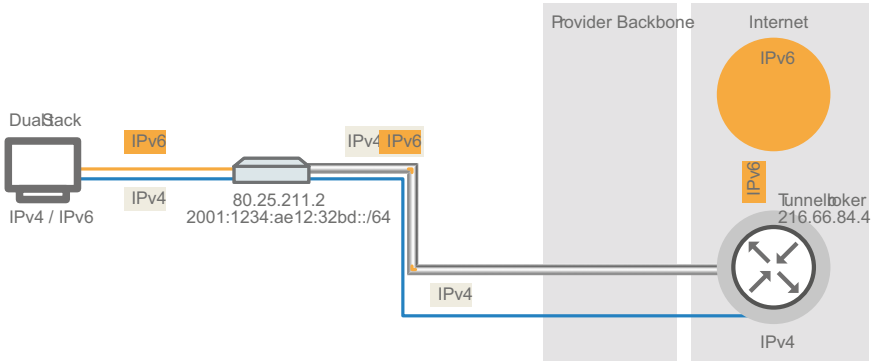
IPv6 is available to networks in a variety of ways. We make a distinction between environments with native IPv6 and those which provide IPv6 through a tunnel.

- **Native IPv6:** Native IPv6 describes a network that communicates to the outside only via IPv6. Users with IPv4 Internet can only gain access to this if the router uses one of the tunnel technologies described below.
- **IPv6 via dual stack:** Dual stack refers to the parallel operation of IPv4 and IPv6 in a network.
- **IPv6 tunneling:** If a router does not have native IPv6 Internet access, it can still access IPv6 networks by means of a tunnel.

12.2 IPv6 Tunneling Technologies

12.2.1 6in4 Tunneling

6in4 tunnels are used to connect two hosts, routers, or to interconnect a host and router. This means that 6in4 tunnels can connect two IPv6 networks via an IPv4 network. The diagram shows a static 6in4 tunnel between the local router and a 6in4 gateway belonging to a tunnel broker.



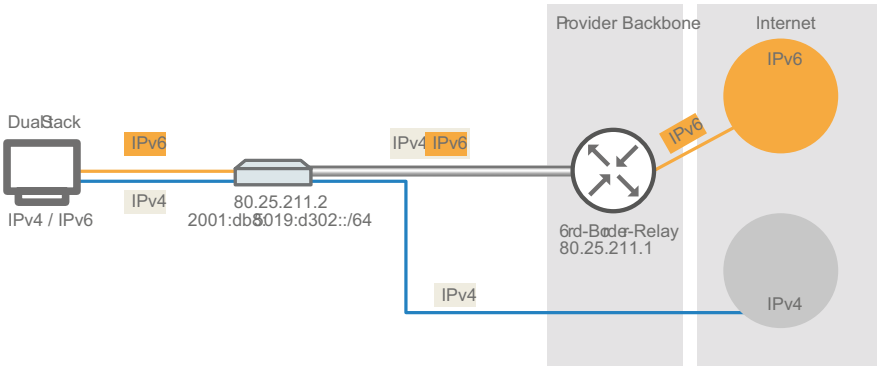
Unlike 6to4, these are dedicated services operated by a known provider. The end-points are fixed and the tunnel broker assigns a static prefix. The advantages of a 6in4 solution are that the gateways are fixed and the operator is known. The fixed prefix from the tunnel broker also determines the number of possible subnets that can be used. A 64-bit prefix (e.g. 2001:db8::/64) allows one subnet to be used. If a 48-bit prefix is used, 16 bits of the 64-bit prefix are available for use. This allows the implementation of up to 65,536 subnets.

The disadvantage of the 6in4 technology is the higher administrative effort. You must be registered with and login to the tunnel broker. In addition, the tunnel endpoints must be statically configured. Where a dynamic IPv4 address is used, the relevant data must be updated regularly. This can be automated by running a script on a router.

6in4 is a relatively secure and stable technology for providing IPv6 Internet access. This technology is thus suitable for operating web servers that are to be accessed over IPv6. The only drawback is the increased effort in administration. This technology is also suitable for professional use.

12.2.2 6rd Tunneling

6rd (rapid deployment) is a development of 6to4. The underlying function is identical. The difference is that just one particular relay is used, as operated by a provider. This solves the two basic problems of the 6to4 technology—the lack of security and stability. The prefix with 6rd is ??either configured manually or sent via DHCP (IPv4), which further reduces the effort involved with configuration. The diagram is a schematic representation of a 6rd scenario.

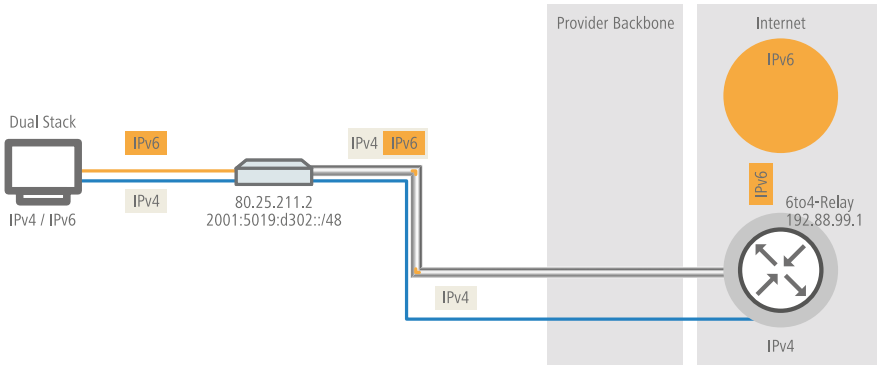


The provider assigns the router with a prefix (2001:db8::/32), which the router then supplements with its own IPv4 address. The IPv6 address generated in this way has the form: 2001:db8:5019:d302::/64. This makes 6rd interesting from two perspectives. The provider has a simple way to give its customers access to the IPv6 Internet. In addition, customers benefit from greatly simplified usage. They do not have to accept the security risks of 6to4, nor do they have to handle the complicated configuration of 6in4.

12.2.3 6to4 Tunneling

6to4 tunneling offers you an easy way to set up a data connection between two IPv6 networks via an IPv4 network. To this end, what is known as a 6to4 tunnel is set up:

- A router between a local IPv6 network and an IPv4 network serves to mediate between the networks.
- The router has both a public IPv4 address and an IPv6 address. The IPv6 address consists of an IPv6 prefix and the IPv4 address in hexadecimal notation. If a router has the IPv4 address 80.25.211.2, this will first be converted into hexadecimal notation: 5019:d302. Supplementing this is an IPv6 prefix (e.g. 2002::/16), so that the IPv6 address for the router appears as follows: 2002:5019:d302::/48.
- If a device in the IPv6 network sends data packets via the router to an IPv4 destination address, then the router first of all repacks the IPv6 packets and encapsulates them into a package with an IPv4 header. The router then forwards the encapsulated package to a 6to4 relay. The 6to4 relay unpacks the packet and forwards it to the desired destination. The following illustration shows the operating principle of 6to4 tunneling:



6to4 tunnels provide a dynamic data connection between IPv6 and IPv4 networks: The reply packets could be routed back using a different 6to4 relay as the one used on the way out. 6to4 tunnels are not a point-to-point connection. For every new data connection, the router always looks for the "nearest" public 6to4 relay. This is done using the anycast address 192.88.99.1. This aspect is an advantage of 6to4 tunneling on the one hand, but it also presents a disadvantage on the other. Public 6to4 relays do not require registration and are freely accessible. What's more, the dynamic data connection is easily configured. In this way it is possible for any user to create a 6to4 tunnel over a public relay, quickly and easily.

On the other hand, the dynamic data connection means that the user has no influence on the choice of the 6to4 relay. The provider of the relay is able to intercept or manipulate data.

12.3 DHCPv6

Compared to IPv4, clients in an IPv6 network do not require automatic address assignment from a DHCP server because they use auto-configuration. However, because certain information such as DNS server addresses are not transmitted during auto-configuration, certain application scenarios can benefit from a DHCP service on the IPv6 network.

12.3.1 DHCPv6 Server

The use of a DHCPv6 server is optional for IPv6. In principle, a DHCPv6 server supports two modes:

- **Stateless**: The DHCPv6 server does not distribute addresses but only information, such as DNS server addresses. Using this method, clients generate their own IPv6 addresses by 'stateless address auto-configuration (SLAAC)'. This method is particularly attractive e.g., for small networks in order to keep administration efforts to a minimum.
- **Stateful**: The DHCPv6 server distributes IPv6 addresses, similar to IPv4. This method is more complicated, since a DHCPv6 server has to assign and manage the addresses.

A DHCPv6 server distributes only the options that are explicitly requested by an IPv6 client, i.e. the server only assigns an address to a client if it explicitly requests one.

Additionally, the DHCPv6 server can pass on prefixes to routers for further distribution. This method is referred to as 'prefix delegation'. A DHCPv6 client must have explicitly requested this prefix, however.

12.3.2 DHCPv6 Client

The auto-configuration available with IPv6 networks makes it very easy and convenient to configure the clients.

However, in order for a client to receive additional information, such as a DNS server address, you must configure the device so that it can activate the DHCPv6 client when necessary.

The settings for the DHCPv6 client ensure that a device receiving certain flags in the router advertisement will start the DHCPv6 client, which can then send requests to the DHCPv6 server:

- **M flag**: If an appropriately configured device receives a router advertisement with the 'M flag' set, the DHCPv6 client will request an IPv6 address from the DHCPv6 server along with other information such as DNS server, SIP server and NTP server.
- **O flag**: With an 'O flag', the DHCPv6 client requests the DHCPv6 server for information such as a DNS server, SIP server and NTP server only, but not an IPv6 address.

Hinweis: If the 'M-flag' is set, the 'O-flag' does not necessarily have to be set as well.

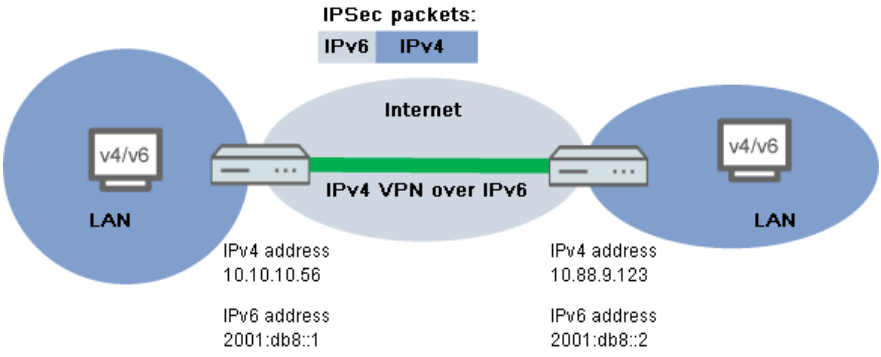
Hinweis: With IPv6, the default route is distributed via router advertisements and not via DHCPv6.

12.4 IPv4 VPN Tunnel via IPv6

Until now it was not possible to set up a VPN between two remote stations using private IPv4 addresses to access the Internet (e.g. 3G/4G networking).

This restriction no longer exists with IPv6, because every IPv6 device receives a public IPv6 address. Thus IPv6 can be used to set up an IPv4 VPN tunnel to interconnect two remote IPv4 networks, regardless of the IPv4 WAN addresses used at each site.

In the example shown, two local IPv4 networks are connected via an IPv4 VPN tunnel, which is established over an IPv6 Internet connection. The IPv4 VPN packets are given IPv6 headers and sent to the remote site via the IPv6 Internet connection (either native or via tunnel broker).



12.4.1 Setup Wizard: IPv4 VPN Tunnel via IPv6 Setup

The Setup Wizard option "Connect two local area networks" helps you to set up a VPN connection.

☐ Start the Hirschmann LANconfig.

LANconfig now automatically searches the local network for devices. As soon as LANconfig has completed its search, it presents a list of all the devices it found, if possible with a brief description, the IP address and the status.

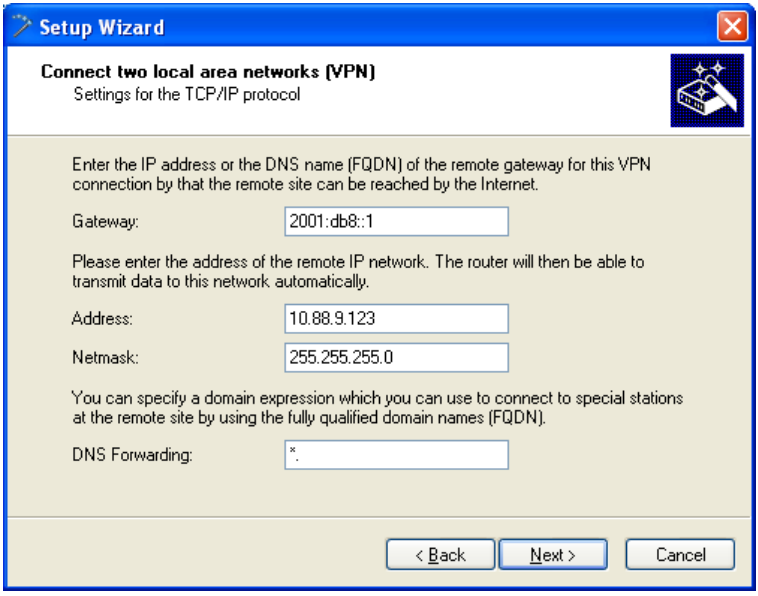
☐ Choose your device from the selection window in LANconfig and select the „Setup Wizard “button or use the menu under `Tools:Setup Wizard`.

LANconfig first reads out the device configuration and then displays the selection window with the optional applications.

☐ Launch the action „Connect two local area networks“.

☐ Follow the Wizard’s instructions and enter the necessary data.

☐ As the gateway address, enter the IPv6 address of the gateway.


Setup Wizard
Connect two local area networks (VPN)
Settings for the TCP/IP protocol
Enter the IP address or the DNS name (FQDN) of the remote gateway for this VPN connection by that the remote site can be reached by the Internet.
Gateway:
2001:db8::1
Please enter the address of the remote IP network. The router will then be able to transmit data to this network automatically.
Address:
10.88.9.123
Netmask:
255.255.255.0
You can specify a domain expression which you can use to connect to special stations at the remote site by using the fully qualified domain names (FQDN).
DNS Forwarding:
*.
< Back
Next >
Cancel

☐ You can then close the Wizard with „Finish“.

The Setup Wizard writes the configuration to the device.

12.5 IPv6 Firewall

12.5.1 Function

While the IPv4 firewall only controls the forwarding of IP data, the IPv6 firewall also regulates the functions of the access lists for all IPv6 server services. Therefore, the IPv6 firewall is similar to a classic firewall design, which separately supports the inbound and outbound communications, as well as forwarding. Since the OpenBAT device configuration specifically controls communication, HiLCOS does not require an outbound firewall.

12.5.2 Configuration

The configuration of the IPv6 firewall is practically the same as the IPv4 firewall; however, it is performed separately.

The inbound and forwarding firewalls each have their own rule tables, which are similar in scope and structure to the IPv4 firewall.

The rules are sorted with decreasing priority, i.e. the rule with the highest priority is at the top of the list. Rules of the same priority are sorted by their precision, analogous to the IPv4 procedure. If a rule requires further actions, these are also performed by firewall in sequence. Otherwise, firewall filtering is terminated after the current rule has been applied.

12.5.3 Default Entries for the IPv6 Firewall Rules

By default, IPv6 firewall has a number of filter rules that are applied on incoming data streams.

Default Entries for the Inbound Rules

This table contains the rules that the firewall will apply to inbound connections. The factory settings provide the following rules for the most important applications:

- **ALLOW-ICMP, ACCEPT**:
  Allow all connections using ICMPV6.
- **ALLOW-DHCP-CLIENT, ACCEPT**:
  Allow communication with the DHCPv6 client.
- **ALLOW-DHCP-SERVER, ACCEPT**:
  Allow communication with the DHCPv6 server.
- **ALLOW-CONFIG-LOCALNET, ACCEPT**:
  Allow configuration in the local network via HTTP, HTTPS, SNMP, SSH, TELNET, TFTP.
- **ALLOW-VPN-CONFIG, ACCEPT-VPN**:
  Allow HTTP, HTTPS, SNMP, SSH, TELNET, and TFTP communication via VPN.
- **ALLOW-DNS-SERVER, ACCEPT**:
  Allow communication with the internal DNS server from the local network.
- **ALLOW-DNS-SERVER-VPN, ACCEPT-VPN**:
  Allow communication with the internal DNS server via VPN.
- **DENY-ALL, REJECT-SNMP**:
  Block all communication and inform the admin via SNMP.

- **ALLOW-CONFIG-WAN, ACCEPT**:
  Allow communication via the WAN interface via HTTPS, SSH. (disabled)
- **ALLOW-IPSEC, ACCEPT**:
  Allow all VPN communication over IPSec. (disabled)
- **ALLOW-IPSEC-HTTPS-ENCAPSULTION, ACCEPT**:
  Allow the use of IPSec over HTTPS. (disabled)

Default Entries for the Forwarding Rules

This table contains the rules that the firewall will apply for forwarding data. The factory settings provide the following rules for the most important applications:

- **ALLOW-VPN, ACCEPT-VPN**:
  Allow all data connections using IPSec.
- **DENY-ALL, REJECT-SNMP**:
  Block all communication via SNMP.
- **ALLOW-OUTBOUND, ACCEPT-VPN**:
  Allow all outbound communication.

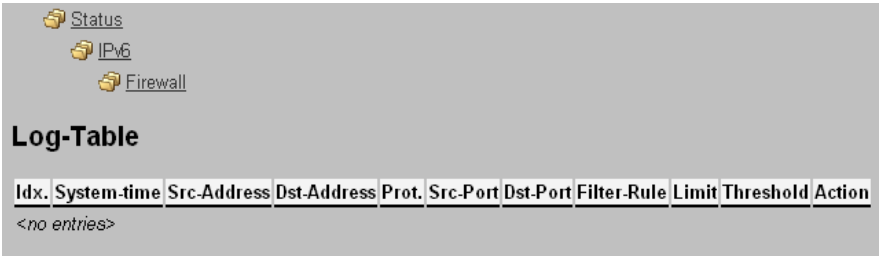
12.5.4 IPv6 Firewall Log Table

Similar to the IPv4 firewall, the IPv6 firewall provides a log table of events in the IPv6 environment.

The syntax of the log table is the same as the IPv4 log table with the exception of the IP address format (IPv6 addresses are in hexadecimal format, IPv4 in decimal format).

Analyzing the IPv6 Firewall Log Table with WEBconfig

You can open IPv6 log tables in WEBconfig with `HiLCOS menu tree:Status:IPv6:Firewall:Log table`.



The items have the following meanings:

- „Idx.“: Sequential index. Furthermore, the table can also be checked via SNMP.
- „System time“: System time in UTC encoding (converted to plain text for display).
- „Source address“: Source address of the filtered packet.
- „Destination address“: Destination address of the filtered packet
- „Prot.“: Protocol (TCP, UDP, etc.) of the filtered packets.
- „Source port“: Source port of the filtered packet (only for port related protocols).
- „Destination port“: Destination port of the filtered packet (only for port related protocols).
- „Filter rule“: Name of the rule that created the entry.
- „Limit“: Bit field containing the description of the limit that caused the firewall to apply the filter. There following values are currently defined:
  - 0x01: Absolute number
  - 0x02: Number per second
  - 0x04: Number per minute
  - 0x08: Number per hour:
  - 0X10: Global limit
  - 0x20: Byte limit (if not set, it is a packet limit)
  - 0x40: Limit only applies in the inbound direction
  - 0x80: Limit only applies in the outbound direction

- „Threshold“:Threshold limit value of the triggering limit.
- „Action“: Bit field which lists all the actions performed. There following values are currently defined:
  - 0x00000001: Accept
  - 0x00000100: Reject
  - 0x00000200: Establish filter
  - 0x00000400: Internet (default router) filter
  - 0x00000800: Drop
  - 0x00001000: Disconnect
  - 0x00004000: Lock source address
  - 0x00020000: Lock destination address and port
  - 0X20000000: Send SYSLOG notification message
  - 0x40000000: Send SNMP trap
  - 0x80000000: Send e-mail

Hinweis: All firewall actions also appear in the IP router trace .

Analyzing the IPv6 Firewall Log Table with LANmonitor

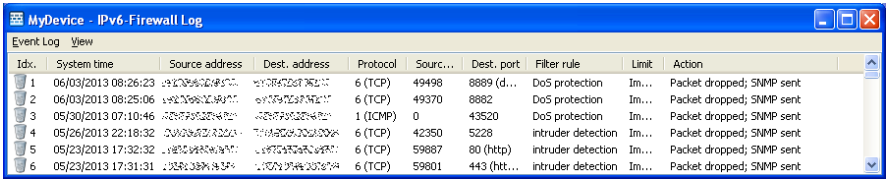
You can view the IPv6 log for a specific device in the LANmonitor.

Do this by starting LANmonitor from the link in the Windows Start menu. You can also launch the LANmonitor for a specific device with the context menu in LANconfig or with the keyboard shortcut `Ctrl + M`.

Via `Device:View firewall event log` you can view the firewall events for a selected device. The firewall events show the last 100 actions of the firewall with the following details:

- „Idx“
- „Timestamp“
- „Src address“
- „Dst address“
- „Protocol“

- „Src port“
- „Dst port“
- „Firewall rule“
- „Limit“
- „Action“


MyDevice - IPv6-Firewall Log
Event Log View
Idx. System time Source address Dest. address Protocol Sourc... Dest. port Filter rule Limit Action
1 06/03/2013 08:26:23 6 (TCP) 49498 8889 (d... DoS protection Im... Packet dropped; SNMP sent
2 06/03/2013 08:25:06 6 (TCP) 49370 8882 DoS protection Im... Packet dropped; SNMP sent
3 05/30/2013 07:10:46 1 (ICMP) 0 43520 DoS protection Im... Packet dropped; SNMP sent
4 05/26/2013 22:18:32 6 (TCP) 42350 5228 intruder detection Im... Packet dropped; SNMP sent
5 05/23/2013 17:32:32 6 (TCP) 59887 80 (http) intruder detection Im... Packet dropped; SNMP sent
6 05/23/2013 17:31:31 6 (TCP) 59801 443 (htt... intruder detection Im... Packet dropped; SNMP sent

12.6 Additional Command-line Commands

Various IPv6 functions can be queried at the command line. The following command-line functions are available:

- „IPv6 Addresses“: `show ipv6-adresses`
- „IPv6 Prefixes“: `show ipv6-prefixes`
- „IPv6 Interfaces“: `show ipv6-interfaces`
- „IPv6 Neighbor Cache“: `show ipv6-neighbour-cache`
- „IPv6 DHCP Server“: `show dhcp6-server`
- „IPv6 DHCP Client“: `show dhcpv6-client`
- „IPv6 Route“: `show ipv6-route`

Additionally, IPv6 communications can be followed with the `trace` command (see page 761).

12.6.1 IPv6 Addresses

The command `show ipv6-addresses` shows a list of IPv6 addresses that are currently being used. This is sorted by interface. Note that an interface can have multiple IPv6 addresses. One of these addresses is always the link-local address, which starts with `fe80::`.

The output is formatted as follows:

<Interface> :

<IPv6 address>, <status>, <attribute>, (<type>)

Tab. 3: Components of the Command-line Output show ipv6-addresses:

Output	**Comment**
Interface	The name of the interface
IPv6 address	The IPv6 address
Status	The status field can contain the following values: ▶ TENTATIVE Duplicate Address Detection (DAD) is currently checking the address. It is not yet available for unicast. ▶ PREFERRED The address is valid ▶ DEPRECATED The address is still valid, but it is being discontinued. The optimal status for communication is PREFERRED. ▶ INVALID The address is invalid and cannot be used for communication. An address given this status after its lifetime has expired.
Attribute	Shows an attribute of the IPv6 address. Possible attributes are: ▶ None No special attributes ▶ (ANYCAST) This is an anycast address ▶ (AUTO CONFIG) The address was retrieved by auto-configuration ▶ (NO DAD PERFORMED) No DAD is performed
Type	The type of IP address

12.6.2 IPv6 Prefixes

The command `show ipv6-prefixes` displays all known prefixes. These are sorted according to the following criteria:

- **Delegated prefixes:** All prefixes that the router has obtained by delegation.
- **Advertised prefixes:** All prefixes that the router announces in its router advertisements.
- **Deprecated prefixes:** All prefixes that are being discontinued. These may still be functional, but they will be deleted after a certain time.

12.6.3 IPv6 Interfaces

The command `show ipv6-interfaces` displays a list of IPv6 interfaces and their status.

The output is formatted as follows:

<Interface> : <Status>, <Forwarding>, <Firewall>

Tab. 4: Components of the Command-line Output show ipv6-interfaces:

Output	Comment
Interface	The name of the interface
Status	The status of the interface Possible entries are: ▶ oper status is up ▶ oper status is down
Forwarding	The forwarding status of the interface. Possible entries are: ▶ forwarding is enabled ▶ forwarding is disabled
Firewall	The status of the firewall. Possible entries are: ▶ forwarding is enabled ▶ firewall is disabled

12.6.4 IPv6 Neighbor Cache

The command `show ipv6-neighbor-cache` displays the current neighbor cache.

The output is formatted as follows:

<IPv6 address> iface <interface> lladdr <MAC address> (<switch port>) <device type> <status> src <source>

Tab. 5: Components of the Command-line Output show ipv6-neighbor-cache:

Output	Comment
IPv6 address	The IPv6 address of the neighboring device
Interface	The interface where the neighbor is accessed
MAC address	The MAC address of the neighbor
Switch port	The switch port on which the neighbor was found
Device type	Neighbor's device type (host or router)
Status	The status of the data connection to neighboring devices. Possible entries are: ▶ INCOMPLETE Resolution of the address was still in progress and the link-layer address of the neighbor was not yet determined. ▶ REACHABLE The neighbor was reached in the last 10 seconds. ▶ STALE The neighbor is no longer qualified as REACHABLE, but an update will only be performed when an attempt is made to reach it. ▶ DELAY The neighbor is no longer qualified as REACHABLE, but data was recently sent to it; waiting for verification by other protocols. ▶ PROBE The neighbor is no longer qualified as REACHABLE. Neighbor solicitation probes are sent to it to confirm availability.
Source	The IPv6 address at which the neighbor was detected.

12.6.5 IPv6 DHCP Server

The command `show dhcpv6-server` displays the current status of the DHCP server. The display includes information about the interface on which the server is active, which DNS server and prefixes it has, and what client preferences it has.

12.6.6 IPv6 DHCP Client

The command `show dhcpv6-client` displays the current status of the DHCP client. The display includes information about the interface being used by the client and the prefixes and DNS server that it is using.

12.6.7 IPv6 Route

The command `show ipv6-route` displays the complete IPv6 routing table. Routers with fixed entered routes are displayed with the suffix [static] and the dynamically obtained routes have the suffix [connected]. The loopback address is marked [loopback]. Other automatically generated addresses have the suffix [local].

12.6.8 Release IPv6 Address

Tab. 6: Command for IPv6 address release

Command	Description
Release [-x] <Interface 1> ... <Interface n>	The DHCPv6 client returns its IPv6 address and/or its prefix to the DHCPv6 server. It then submits a new request for an address or prefix to the DHCPv6 server. Depending on the provider, the server assigns a new address to the client, or reassigns the previous one. Whether the client receives a different address or prefix is determined solely by the server. The option switch `-x` suppresses the confirmation message. The `*` wildcard applies the command on all of the interfaces and prefix delegations.

12.6.9 Overview of Parameters

Hinweis: The traces available for a particular model can be displayed by entering `trace` without any arguments.

Tab. 7: Overview of Trace Parameters

This parameter ...	...causes the following message in the trace:
Status	Data connection status messages
Error	Data connection error messages
IPX router	IPX routing
PPP	PPP protocol negotiation
SAP	IPX service advertising protocol
IPX watchdog	IPX watchdog spoofing
SPX watchdog	SPX watchdog spoofing
LCR	Least-cost router
Script	Script negotiation
IPX RIP	IPX routing information protocol
Firewall	Displays firewall events
RIP	IP routing information protocol
ARP	Address resolution protocol
ICMP	Internet control message protocol
IP Masquerading	Events in the masquerading module

Tab. 7: Overview of Trace Parameters

This parameter ...	**...causes the following message in the trace:**
DHCP	Dynamic host configuration protocol
NetBIOS	NetBIOS administration
DNS	Domain name service protocol
Packet dump	Displays the first 64 bytes of a packet in hexadecimal
D channel dump	Traces the D channel of the ISDN bus connected
ATM cell	ATM packet level
ATM error	ATM error
ADSL	ADSL link status
SMTP client	Email processing with the integrated mail client
Mail client	Email processing with the integrated mail client
SNTP	Simple network time protocol
NTP	Time server trace
Connact	Messages from the activity protocol
Cron	Activities of the scheduler (cron table)
RADIUS	RADIUS trace
Serial	Information on the state of the serial interface
USB	Information on the state of the USB interface
Load balancer	Information on load balancing
VRRP	Information about the virtual router redundancy protocol
Ethernet	Information on the Ethernet interfaces
VLAN	Information on virtual networks
IGMP	Information about the Internet group management protocol
WLAN	Information on activity in the wireless networks
IAPP	Trace of the inter-access point protocol, displays information about WLAN roaming.
DFS	Trace on dynamic frequency selection, automatic channel selection in the 5 GHz wireless LAN band
Bridge	Information on the wireless LAN bridge
EAP	Trace on EAP, the key negotiation protocol used with WPA/802.11i and 802.1x
Spgtree	Information on the spanning tree protocol
LANAUTH	LAN authentication (e.g. Public Spot)
SIP-Packet	SIP information that is exchanged between a VoIP router and a SIP provider or a upstream SIP telephone system
VPN status	IPSec and IKE negotiations
VPN packet	IPSec and IKE packets
XML-Interface-PbSpot	Messages from the Public Spot XML interface
IPv6 config	Information on the IPv6 configuration
IPv6 firewall	IPv6 firewall events
IPv6-Interfaces	Information about the IPv6 interfaces
IPv6-LAN-Packet	Data packets over the IPv6 LAN connection
IPv6-Router	Information about the IPv6 routing
IPv6-WAN-Packet	Data packets over the IPv6 WAN connection

12.7 Enhancements to LANconfig

12.7.1 IPv6 configuration menu

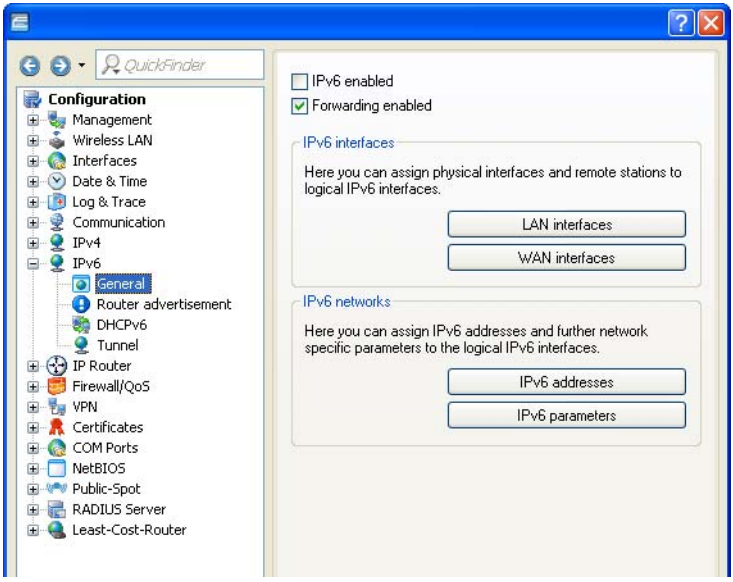
Where previous versions provided configuration menus for TCP/IP for IPv4, you now find the options „IPv4“ and „IPv6“.

Click on „IPv6“ to adjust the settings for this protocol. The configuration dialog „IPv6“ is divided into the options „General“, „Router advertisement“ and „Tunnel“. By default a click on „IPv6“ takes you straight to the „General“ options.

- General

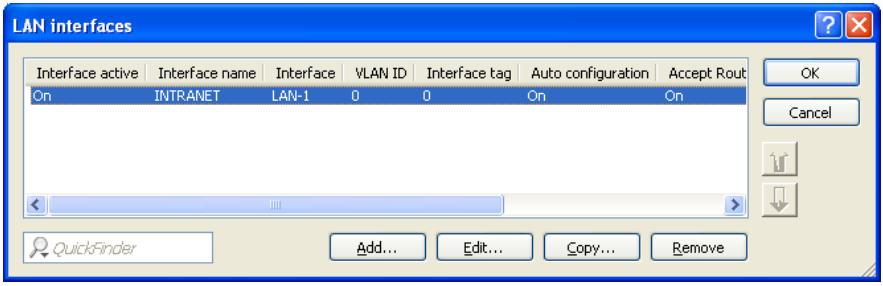
  This is where you make the basic settings.

  - „IPv6 enabled:“ This is where you can enable or disable IPv6 for the device.
  - „Forwarding enabled:“ Forwarding is used for packet forwarding between IPv6 interfaces. This option is activated by default.



- The buttons „LAN interfaces“ and „WAN interfaces“ access the tables where you can add new interfaces, configure existing interfaces, or delete them.

For each existing IPv4 network, you must create an equivalent IPv6 network under „LAN interfaces“. Here, the settings for interface binding, routing tag, and VLAN ID must match the settings of the corresponding IPv4 network settings. Because a device can have multiple IPv6 addresses, you must add statically configured IPv6 addresses under „IPv6 addresses“.



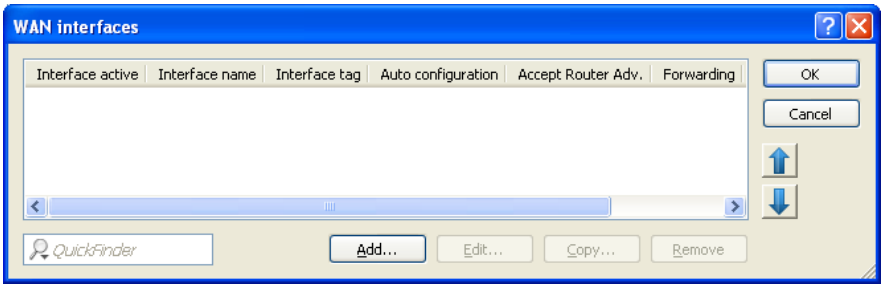
Entries in the „LAN interfaces“ table have the following meaning:

- „Interface active“: Activates or deactivates this LAN interface.
- „Interface name“ or „Network name“: Enter a name for the logical IPv6 interface which is to apply to the physical interface (interface assignment) and the VLAN ID.
- „Interface“: Select the physical interface to be combined with the VLAN ID to form the logical IPv6 interface. With IPv6, the mapping "any" used with IPv4 is no longer possible.
- „VLAN ID“: Select the VLAN ID to be combined with the physical interface to form the logical IPv6 interface.
- „Interface tag“: The interface tag that you enter here is a value that uniquely identifies the network. All packets received by this device on this network will be internally marked with this tag. The interface tag enables the routes which are valid for this network to be separated even without explicit firewall rules.
- „Autoconfiguration“: Enable or disable the automatic configuration of addresses (SLAAC or DHCPv6) for this interface in the client role.

  Hinweis: If the device itself sends router advertisements from this interface, it does not produce IPv6 addresses from received router advertisements from other routers, even when auto-configuration is enabled.

- „Accept router advertisements“: Enables or disables the processing of received router advertisement messages. With processing disabled, the device ignores any prefix, DNS and router information received via router advertisements.
- „Forwarding“: Enables or disables the forwarding of data packets to other interfaces. With forwarding disabled, no router advertisements are transmitted from this interface.
- „MTU“: Here you set the valid MTU for the corresponding link.
- „Firewall“: If the global firewall is enabled for IPv6 interfaces, you can disable the firewall for an individual interface here.
- „Comment“: Enter a descriptive comment for this entry.

For each remote station with which you want to communicate using IPv6, you must additionally create an equivalent logical IPv6 WAN interface under „WAN interfaces“. The name of the IPv6 WAN interface must match the name of the IPv4 remote station.

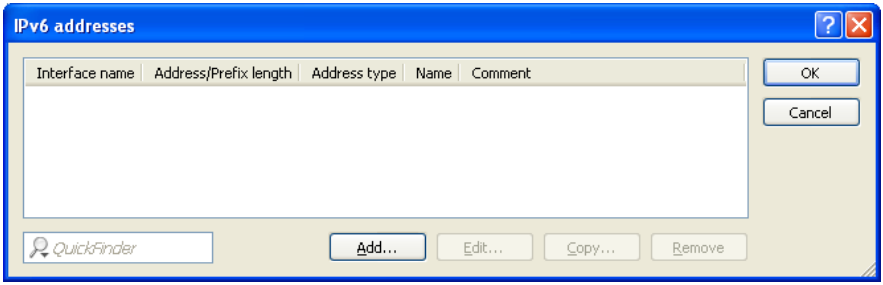


Entries in the „WAN interfaces“ table have the following meaning:

- „Interface active“: Activates or deactivates this WAN interface.
- „Interface name“: The name of the logical IPv6 interface must match that of the corresponding IPv4 connection.
- „Interface tag“: The interface tag that you enter here is a value that uniquely identifies the network. All packets received by this device on this network will be internally marked with this tag. The interface tag enables the routes which are valid for this network to be separated even without explicit firewall rules.
- „Autoconfiguration“: Enable or disable the automatic configuration of addresses (SLAAC or DHCPv6) for this interface in the client role.
- „Accept router advertisements“: Enables or disables the processing of received router advertisement messages. With processing disabled, the device ignores any prefix, DNS and router information received via router advertisements.
- „Forwarding“: Enables or disables the forwarding of data packets to other interfaces. With forwarding disabled, no router advertisements are transmitted from this interface.
- „Firewall“: If the global firewall is enabled for IPv6 interfaces, you can disable the firewall for an individual interface here.
- „Comment“: Enter a descriptive comment for this entry.

The buttons „IPv6 addresses“ and „IPv6 parameters“ are used to assign IPv6 addresses to interfaces and to configure the interface parameters (gateway address, primary and secondary DNS).

The „IPv6 addresses“ table is used to create IPv6 addresses for LAN and WAN interfaces.



Entries in the „IPv6 addresses“ table have the following meaning:

- „Interface name“: Give a name to the interface that you want to assign the IPv6 network.
- „Address/prefix length“: Specify an IPv6 address including the prefix length for this interface.

  The default prefix length is ?64 bits ("/64")?. If possible do not use IPv6 addresses with longer prefixes, as many IPv6 mechanisms in the device (e.g. autoconfiguration) are designed for a maximum length of 64 bits.

  Example:

  - Global unicast address: "2001:db8::1/64"
  - Unique local address: "fd00::1/64"

  Hinweis: Link-local addresses are fixed and not configurable.

- „Address type“: Specify the type of IPv6 address.

Options:

- Unicast
- Anycast
- EUI-64

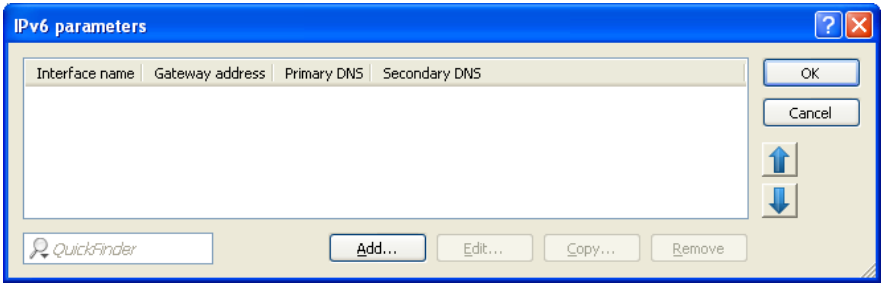
With the address type EUI-64, IPv6 addresses conform to the IEEE standard "EUI-64". The MAC address of the interface thus forms a uniquely identifiable part of the IPv6 address. The correct input format for an IPv6 address including the prefix length as per EUI-64 would be: "2001:db8:1::/64". "EUI-64" ignores any value set as interface identifier in the corresponding IPv6 address and replaces it with an interface identifier as per "EUI-64". The prefix length for "EUI-64" must be "/64".

With the Unicast address type, you use the „Address/prefix length“ field to specify a full IPv6 address along with its interface identifier, e.g. "2001:db8::1234/64".

With the Anycast address type, you can also use the „Address/prefix length“ field to specify a full IPv6 address along with its interface identifier, e.g. "2001:db8::1234/64". Internally, the device handles this address as an anycast address.

- „Name“: Enter a descriptive name for this combination of IPv6 address and prefix.
- „Comment“: Enter a descriptive comment for this entry.

The table „IPv6 parameters“ is used to manually configure static parameters for LAN or WAN interfaces, IPv6 DNS servers, and IPv6 gateways if you choose not to use autoconfiguration or DHCPv6.



Entries in the „IPv6 parameters“ table have the following meaning:

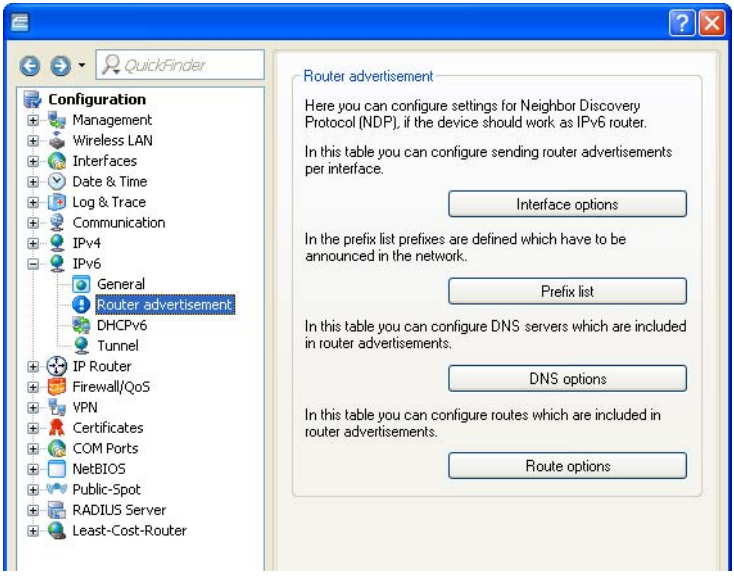
- „Interface name“: Give a name to the interface for which the IPv6 parameters are to be configured.
- „Gateway address“: Specify the IPv6 gateway to be used by this interface.

  Hinweis: This parameter overrides gateway information that the device may receive via router advertisements, for example.

- „Primary DNS“: Specify the primary IPv6 DNS server to be used by this interface.
- „Secondary DNS“: Specify the secondary IPv6 DNS server to be used by this interface.

Router Advertisement

The „Router advertisement“ configuration provides you with four buttons for setting up the Neighbor Discovery Protocol (NDP) if the device is to operate as an IPv6 router:



Each button opens a table with the settings for the corresponding function:

Interface options:

Here you can enable or disable the following interface functions:

☐ „Send router advertisement“
Controls the periodic transmission of router advertisements and the response to router solicitations.

☐ „Managed flag“
With this function enabled, clients receiving this router advertisement will configure their addresses with stateful autoconfiguration (DHCPv6). Clients then automatically retrieve other information, such as the DNS server.

☐ „Other flag“
If this function is active, a client will attempt to obtain additional information via DHCPv6, such as DNS server addresses. For each prefix, you can specify whether or not a client should form addresses by auto-configuration: Navigate to the „Prefix list“ under „Allow auto-configuration (SLAAC)“.

☐ „Default router“
Defines how the device advertises itself as the default gateway or router. The parameters have the following functions:

- "Automatic": As long as a WAN connection exists, the device sends a positive router lifetime in the router advertisement messages. The result is that a client uses this router as the default gateway.

  If there is no WAN connection, the router sets the router lifetime to "0". A client then stops using this router as the default gateway.

- "Always": The router lifetime is always positive—i.e. greater than "0"—irrespective of the WAN connection status.

- "Never": The router lifetime is always "0".

☐ „Router priority“
Defines the preference of this router. Clients enter this preference into their local routing tables.

Prefix list:

Set the prefix options for the interfaces that are being used. The following settings are possible:

☐ „Prefix“
Enter a prefix that is announced with router advertisements, e.g. "2001:db8::/64". The prefix length must always be exactly "/64", otherwise it will be impossible for clients to generate their addresses by adding their interface identifiers (with a length of 64 bits). If a prefix delegated by the provider is to be propagated automatically, set "::/64" here and enter the name of the corresponding WAN interface as the parameter „Receive prefix from“.

☐ „Subnet ID“
Here you enter the subnet ID that is to be combined with the prefix delegated by the provider. If the provider assigns the prefix "2001:db8:a::/48", for example, and the subnet ID is "0001" (or "1" for short), then the router advertisement on this interface is given the prefix "2001:db8:a:0001::/64". The maximum subnet length with a 48-bit long delegated prefix is ??16 bits (i.e. 65,536 subnets), with available subnet IDs ranging from "0000" to "FFFF". With a delegated prefix of "/56", the maximum subnet length is 8 bits (i.e. 256 subnets) with subnet IDs ranging from "00" to "FF". In general, the subnet ID "0" is used when the WAN IPv6 address is formed automatically. This is why subnet IDs for LANs start at "1". The default setting is "1".

☐ „Allow auto-configuration (SLAAC)“
Specifies whether the prefix is to be used for a stateless address autoconfiguration (SLAAC). The default setting is "enabled".

☐ „Receive prefix from“
Specifies the name of the interface used to receive a prefix via DHCPv6 prefix delegation or tunnel. This prefix can be used to derive and propagate a subnet for each interface.

DNS options

Specifies the DNS information in router advertisements according to RFC6106. The following settings are possible:

☐ „Interface name“
Name of the interface on which the IPv6 DNS server announces information in router advertisements.

☐ „Primary DNS“

IPv6 address of the first IPv6 DNS server (recursive DNS server, RDNSS, according to RFC 6106) for this interface.

- ☐ „Secondary DNS“
  IPv6 address of the secondary IPv6 DNS server for this interface.
- ☐ „Import DNS search list from the internal DNS server“
  Indicates whether the DNS search list or the own domain for this logical network should be inserted from the internal DNS server, e.g., "internal". The own domain can be configured under `IPv4:DNS:General settings`. The default setting is "enabled".
- ☐ „Import DNS search list from WAN“
  Specifies whether the DNS search list sent by the provider (e.g., provider-xy.de) is announced in this logical network. This feature is available only if the prefix list is connected to the corresponding WAN interface under „Receive prefix from“.

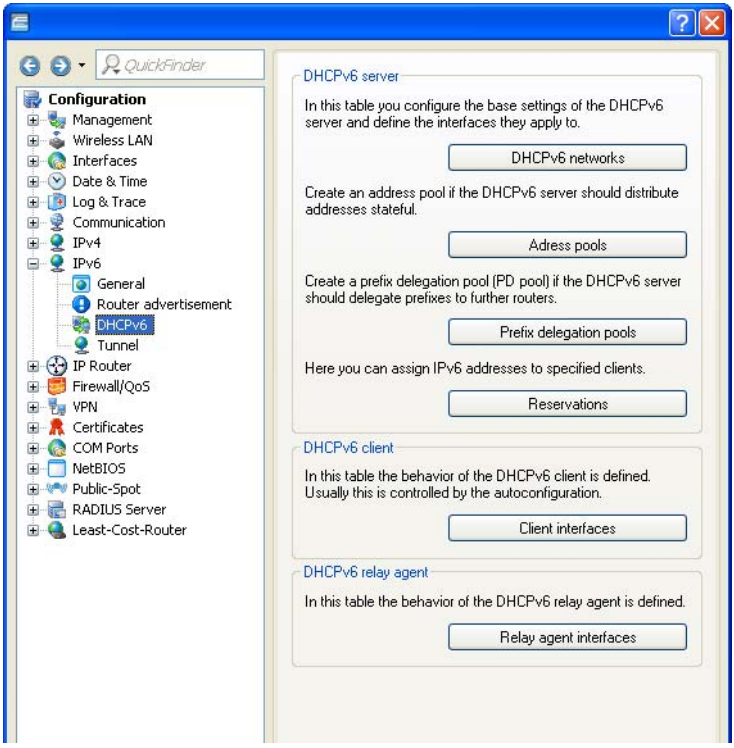
Route options

Specifies the route option in router advertisements according to RFC 4191 (Route Information Option). The following settings are possible:

- ☐ „Interface name“
  Specifies the name of the logical interface to be used for sending router advertisements with this route option.
- ☐ „Prefix“
  Prefix of the route option, e.g."2001:db8::/32".
- ☐ „Route preference“
  The preference of the route. Possible values are "high", "medium" (default) and "low".

DHCPv6

This is where you configure the DHCPv6 server, the DHCPv6 client and the DHCPv6 relay agent.

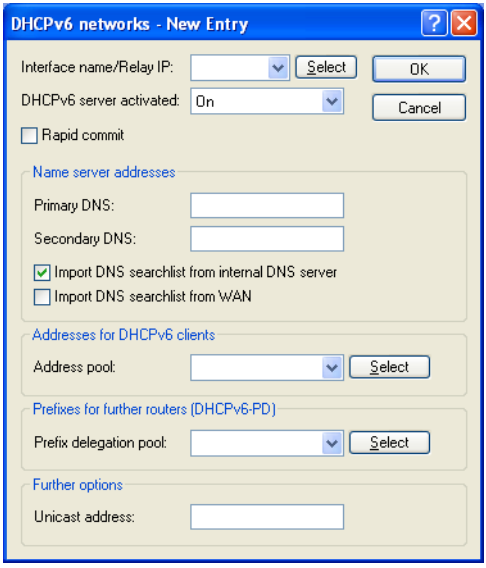


DHCPv6 Server

Use the following buttons to access the tables and adjust the respective functions:

DHCPv6 networks

This table is used to configure the basic settings of the DHCPv6 server, and to specify which interfaces they apply to.



☐ „Interface name or relay“
Name of the interface on which the DHCPv6 server is working, for example "INTRANET". Alternatively, you can also enter the IPv6 address of the remote DHCPv6 relay agent.

☐ „DHCPv6 server activated“
Activates or deactivates the entry.

☐ „Rapid commit“
With rapid commit activated, the DHCPv6 server responds directly to a solicit message with a reply message.

Hinweis: The client must explicitly include the rapid commit option in its solicit message.

☐ „Primary DNS“
IPv6 address of the primary DNS server.

☐ „Secondary DNS“
IPv6 address of the secondary DNS server.

☐ „Import DNS search list from the internal DNS server“

Indicates whether the DNS search list or the own domain for this logical network should be inserted from the internal DNS server, e.g., "internal". The own domain can be configured under `IPv4:DNS:General settings`. The default setting is "enabled".

☐ „Import DNS search list from WAN“
Specifies whether the DNS search list sent by the provider (e.g., provider-xy.de) is announced in this logical network. The default setting is "disabled".

☐ „Address pool“
Name of the address pool used for this interface.

Hinweis: If the DHCPv6 server operates 'stateful' addresses distribution, you must enter the corresponding addresses into the „Address pools“ table.

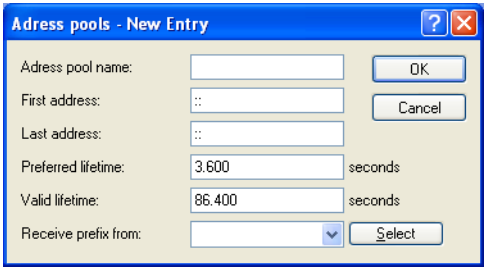
☐ „Prefix delegation pool“
Name of prefix pools to be used by the DHCPv6 server.

Hinweis: If the DHCPv6 server is to delegate prefixes to other routers, you must enter the corresponding prefixes in the table „Prefix delegation pools“.

☐ „Unicast address“
By default the DHCPv6 server exclusively responds to multicast requests. If the DHCPv6 server should respond to a unicast request, this IPv6 address can be configured here. Generally speaking, multicast is sufficient for communication.

Address pools

If distribution of the DHCPv6 server is to be stateful, this table defines an address pool:



- ☐ „Address pool name“
  Name of the address pool
- ☐ „First address“:
  First address in the pool, e.g. "2001:db8::1"
- ☐ „Last address“:
  Last address in the pool, e.g. "2001:db8::9"
- ☐ „Preferred lifetime“
  Here you specify the time in seconds that the client should treat this address as 'preferred'. After this time elapses, a client classifies this address as "deprecated".
- ☐ „Valid lifetime“
  Here you specify the time in seconds that the client should treat this address as 'valid'.

  Hinweis: If you use a prefix from a WAN interface for dynamic address formation, you cannot configure values for `preferred lifetime` and `valid lifetime`. In this case, the device automatically determines the values that apply to the prefix delegated by the provider.

- ☐ „Receive prefix from“
  With this parameter you can assign addresses to the network clients from the prefix that the router retrieved from the WAN interface via DHCPv6 prefix delegation. Select the desired WAN interface here. For example, if the provider assigned the prefix "2001:db8::/64", you can then enter the value "::1" in the parameter „First address“ and "::9" in

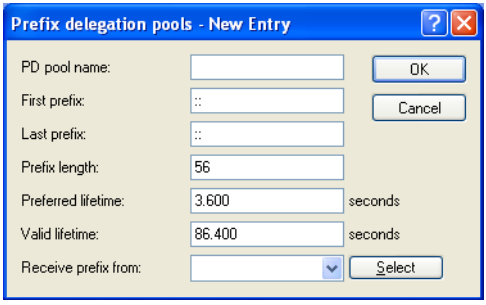
„Last address“. In combination with the prefix "2001:db8::/64" as delegated by the provider, the clients receive addresses from the pool "2001:db8::1" to "2001:db8::9". If the provider prefix is greater than "/64", e.g.,"/48" or "56", you must take subnetting for the logical network in to account in the address. **Example:**

- Assigned provider prefix: "2001:db8:abcd:aa::/56"
- "/64" as the prefix of the logical network (subnet ID 1): "2001:db8:abcd:aa01::/64"
- First address: "0:0:0:0001::1"
- Last address: "0:0:0:0001::9"

Hinweis: You should only use this mechanism if the provider assigns a fixed prefix. Otherwise, it is possible that the provider delegates a new prefix to the router, but the client still has an address from the pool with the old prefix. In this case, the client must update its address at the server.

Prefix delegation pool

In this table, you specify the prefixes that the DHCPv6 server delegates to other routers:



☐ „PD pool name“
Name of the PD pool

☐ „First prefix“
First prefix for delegation in the PD pool, e.g. "2001:db8:1100::"

☐ „Last prefix“
Last prefix for delegation in the PD pool, e.g. "2001:db8:FF00::"

☐ „Prefix length“
Length of the prefixes in the PD pool, e.g. "56" or "60"

☐ „Preferred lifetime“
Here you specify the time in seconds that the client should treat this prefix as 'preferred'. After this time elapses, a client classifies this address as "deprecated".

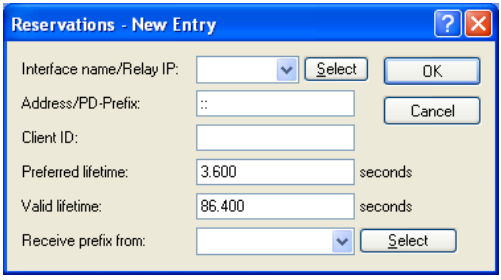
☐ „Valid lifetime“
Here you specify the time in seconds that the client should treat this prefix as 'valid'.

Hinweis: If you use a prefix from a WAN interface for dynamic address formation, you cannot configure values for `preferred lifetime` and `valid lifetime`. In this case, the device automatically determines the values that apply to the prefix delegated by the provider.

☐ „Receive prefix from“
Name of the WAN interface from which the client should use the prefix to form the address or prefix.

Reservations

If you want to assign fixed IPv6 addresses to clients or fixed prefixes to routers, you can use this table to make a reservation for each client.



☐ „Interface name or relay“
Name of the interface on which the DHCPv6 server is working, for example "INTRANET". Alternatively, you can also enter the IPv6 address of the remote relay agent.

☐ „Address/PD prefix“
IPv6 address or PD prefix that you want to assign statically.

☐ „Client ID“
DHCPv6 unique identifier (DUID) of the client.

DHCPv6 clients are no longer identified with their MAC addresses like DHCPv4 clients, they are identified with their DUID instead. The DUID can be read from the respective client, for example, on Windows with the shell command `show dhcpv6-client` or in WEBconfig under `Status:IPv6:DHCPv6:Client:Client ID`.

For devices working as a DHCPv6 server, the client IDs for clients that are currently using retrieved IPv6 addresses are to be found under `Status:IPv6:DHCPv6:Server:Address bindings`, and retrieved IPv6 prefixes are under `Status:IPv6:DHCPv6:Server:PD bindings`.

LANmonitor displays that client IDs under „DHCPv6 server“.

☐ „Preferred lifetime“
Here you specify the time in seconds that the client should treat this address as 'preferred'. After this time elapses, a client classifies this address as "deprecated".

☐ „Valid lifetime“
Here you specify the time in seconds that the client should treat this address as 'valid'.

Hinweis: If you use a prefix from a WAN interface for dynamic address formation, you cannot configure values for `preferred lifetime` and `valid lifetime`. In this case, the device automatically determines the values that apply to the prefix delegated by the provider.

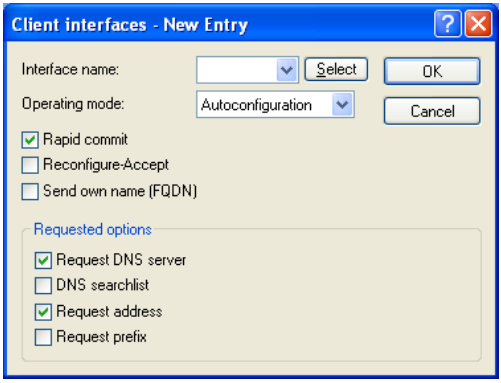
☐ „Receive prefix from“
Name of the WAN interface from which the client should use the prefix to form the address or prefix.

DHCPv6 client

Use the following buttons to access the tables and adjust the respective functions:

Interfaces

This table determines the behavior of the DHCPv6 client.



Hinweis: Normally client behavior is controlled by the auto-configuration. Only make entries in this table if you want to use the client in "stand-alone" mode or if there are other specific options that deviate from the default settings.

☐ „Interface name“
Name of the interface that the DHCPv6 client operates on. These may be LAN interfaces or WAN interfaces (remote stations), such as "INTRANET" or "INTERNET".

☐ „Operating mode“
Determines if and how the device enables the client. Possible values are:

- "Autoconfiguration": The device waits for router advertisements, and then starts the DHCPv6 client. This option is the default setting.
- "Yes": The device starts the DHCPv6 client as soon as the interface is active, without waiting for router advertisements. The device ignores the specifications from router advertisements.
- "No": The DHCPv6 client is disabled on this interface. Even if the device receives router advertisements, it will not start the client.

☐ „Rapid commit“
When rapid commit is activated, the client attempts to obtain an IPv6 address from the DHCPv6 server with just two messages. If the DHCPv6 server is configured correspondingly, it immediately responds to this solicit message with a reply message.

☐ „Reconfigure accept“

If the client successfully negotiates a re-configuration (reconfigure) with the server during first contact, the server can request the client to update its address or other information at any time. The mechanism is protected by the so-called 'Reconfigure Key', so that only the original server with the correct key can make requests to the client. If the client receives a reconfigure message without a valid reconfigure key, the client rejects this invocation. The client supports the "Reconfigure Key Authentication Protocol" according to RFC 3315 for the options "Renew" and "Information Request", and also "Rebind" as per RFC 6644.

This option is enabled by default for WAN interfaces.

☐ „Send own name (FQDN)“
The client sends its own host name (fully qualified domain name). By default, this option is active on LAN interfaces.

☐ „Request DNS server“
Specifies whether the client queries the DHCPv6 server for DNS servers.

Hinweis: You must enable this option in order for the device to obtain information about a DNS server.

☐ „DNS search list“
The client queries the DNS search list.

☐ „Request address“
Determines whether the client should request the DHCPv6 server for an IPv6 address.

Hinweis: Only activate this option if addresses configured by the DHCPv6 server via this interface are stateful, i.e. not distributed by 'SLAAC'.

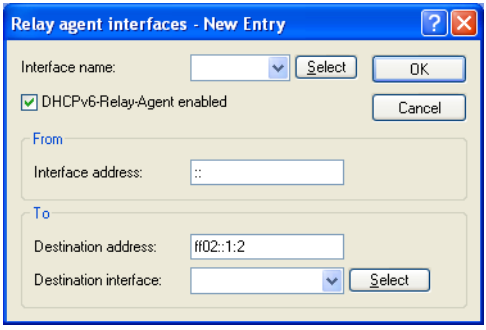
☐ „Request prefix“
Determines whether the client should request the DHCPv6 server for an IPv6 prefix. Activating this option is only necessary if the device itself functions as a router and redistributes these prefixes. This option is enabled by default on WAN interfaces in order for the DHCPv6 client to request a prefix from the provider for use in its local network. This option is disabled by default on LAN interfaces because devices in a local network are more likely to function as clients rather than as routers.

DHCPv6 Relay Agent

Use the following buttons to access the tables and adjust the respective functions:

Interfaces

A DHCPv6 relay agent forwards DHCP messages between DHCPv6 clients and DHCPv6 servers, which are located in different networks. This table determines the behavior of the DHCPv6 relay agent.



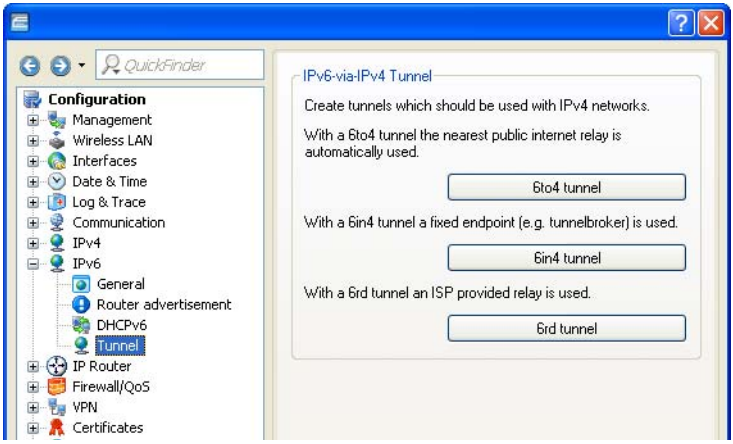
- ☐ „Interface name“
  The name of the interface on which the relay agent receives requests from DHCPv6 clients, e.g. "INTRANET".
- ☐ „Relay agent enabled“
  Determines if and how the device enables the relay agent. Possible values are:
  - ▶ "Yes": Relay agent is enabled. This option is the default setting.
  - ▶ "No": Relay agent is not enabled.
- ☐ „Interface address“
  The relay agent's own IPv6 address at the interface that is configured under Interface Name. This IPv6 address is used as a sender address in DHCP messages that are forwarded. This sender address enables DHCPv6 clients to uniquely identify a relay agent. An explicit specification of the interface address is necessary because an IPv6 host can have multiple IPv6 addresses for each interface.
- ☐ „Dst address“

The IPv6 address of the (destination) DHCPv6 server which the relay agent is to forward DHCP requests to. The address can be either a unicast or link-local multicast address. When using a link-local multicast address, you must specify the destination interface where the DHCPv6 server is to be reached. All DHCPv6 servers and relay agents are available at the link-local multicast address ff02::1:2.

- ☐ „Destination interface“
  The destination interface where the parent DHCPv6 server or the next relay agent is to be reached. This information is essential if a link-local multicast address is configured under the destination address, as link local-multicast addresses are only valid at that respective link.

Tunnel

The „Tunnel “configuration offers you 3 buttons to create IPv6 tunnels that can be used over IPv4 networks. Use these options to gain access to the IPv6 Internet using an IPv4 connection.



- „6to4 tunnel“: This button opens the 6to4 tunnel settings.

  Hinweis: Connections through a 6to4 tunnel work with relays that are selected by the IPv4 Internet provider's backbone. The device administrator has no influence on relay selection. Furthermore, the selected relay can change without the administrator knowing about it. For this reason, data connections via a 6to4 tunnels are suitable **for test purposes only**. In particular, avoid using 6to4-tunnel data connections for productive systems or for the transmission of confidential data.

- „6in4 tunnel“: This button opens the 6in4 tunnel settings.

  Hinweis: 6in4 tunnels require more administrative effort, but they represent a secure and stable technology for IPv6 Internet access. This option is also suitable for professional use.

- „6rd tunnel“: This button opens the 6rd tunnel settings.

  Hinweis: 6rd tunneling is suitable for end users and for professional applications because configuration is less complex than with 6in4 tunneling and the technology avoids the security risks of 6to4 tunneling.

12.7.2 Configuring PPP Negotiation Settings

In the PPP list, you are able to specify you own definition of PPP negotiation for every remote site contacting your network.

You can also specify whether communications should use an IPv4 or an IPv6 connection.

The authentication of point-to-point connections in the WAN commonly relies on one of the protocols PAP, CHAP, MS-CHAP or MS-CHAPv2. The protocols here have a "hierarchy" amongst themselves, i.e. MSCHAPv2 is a "higher-level" protocol than MSCHAP, CHAP and PAP (higher protocols provide higher security). Many dial-in routers at Internet providers allow up-front authentication using a higher-level protocol such as CHAP, but only support the use of PAP further down the line. If the setting for the protocol for authentication is fixed in the relevant device, the data connection may be lost because no common authentication protocol can be negotiated.

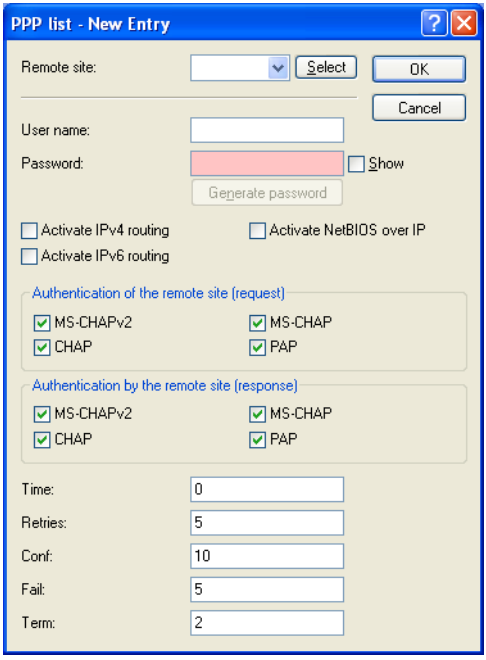
Hinweis: In principle authentication can be repeated while the connection is being negotiated. Another protocol can be selected if, for example, it can only be recognized from the username at the earliest. However, this repeat negotiation is not supported in all scenarios. In particular when dialing in over UMTS, the device must explicitly refuse the provider's request for CHAP to be able to provide PAP user data for requests to be forwarded by the provider.

A flexible setting for the authentication protocols in the device ensures that the PPP connection is established as required. In addition, one or more protocols can be defined that are accepted for authentication of remote sites in the device (inbound data connections) and on login of the device into other remote sites (outbound data connections).

- When establishing inbound data connections, the device requires the lowest of the permitted protocols, but where possible it also permits the remote site to use one of the higher-level protocols (enabled in the device).
- When establishing outbound data connections, the device offers all enabled protocols, but only permits a selection from precisely these protocols. It is not possible to negotiate one of the disabled, possibly higher-level, protocols.

The PPP authentication protocols are set in the PPP list.

LANconfig: `Communication:Protocols:PPP list`

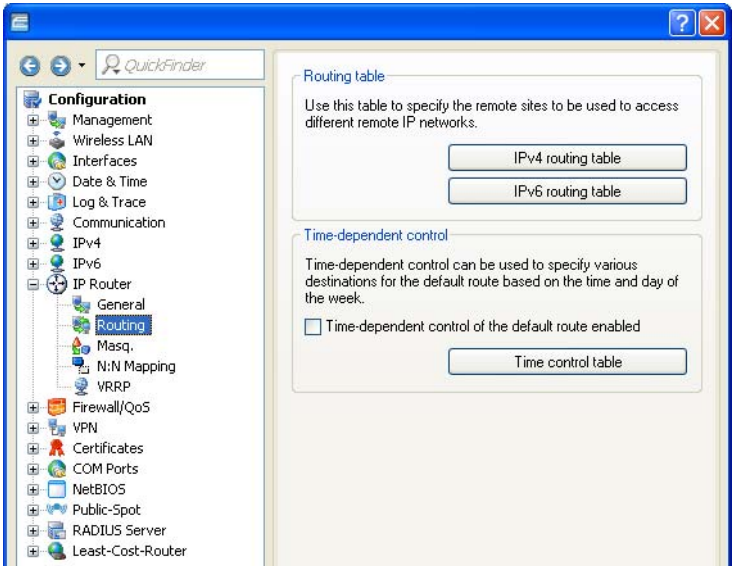


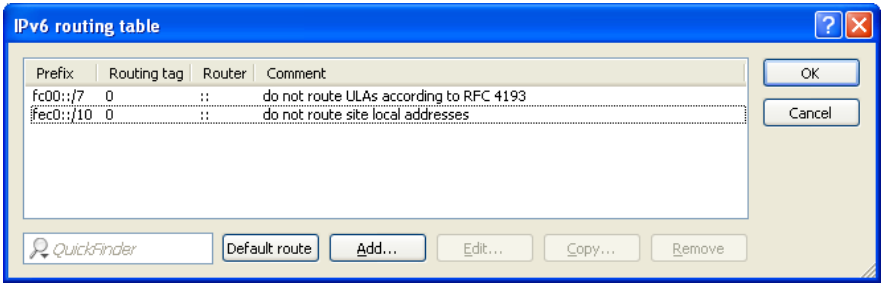
12.7.3 IP Routing Tables

Unlike previous versions where the configuration menu contained just a single IP routing table, this item now offers the configuration of separate routing tables for IPv4 and IPv6 connections.

You will find the new table under `IP router:Routing:IPv6 routing table`

The IPv4 settings that were previously in the table „IP routing table“ are now located in the „IPv4 routing table “.





The table contains the entries to be used for routing packets with IPv6 addresses.

☐ **Prefix**

Specify the prefix of the network area for which the data is to be routed to the given remote station.

☐ **Routing tag**

Specify the routing tag for this route. This route is active only for packets with the same tag. The data packets receive the routing tag either from the firewall or depending on the LAN or WAN interface used.

☐ **Router**

This is where you specify the remote site for this route.

☐ **Comment**

Enter a descriptive comment for this entry.

Hinweis: Entering a comment is optional.

12.7.4 Separate Views for the IPv4 and IPv6 Firewalls

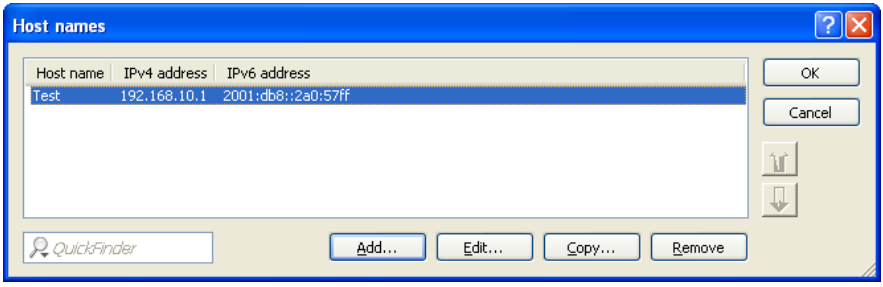
As of HiLCOS version 8.80, you can configure the rules for the IPv4 and IPv6 firewalls in separate views.

The corresponding configurations are located under `Firewall/QoS`IPv4 rules and `Firewall/QoS`IPv6 rules respectively.

12.7.5 IPv6 DNS Hosts in the DNS List

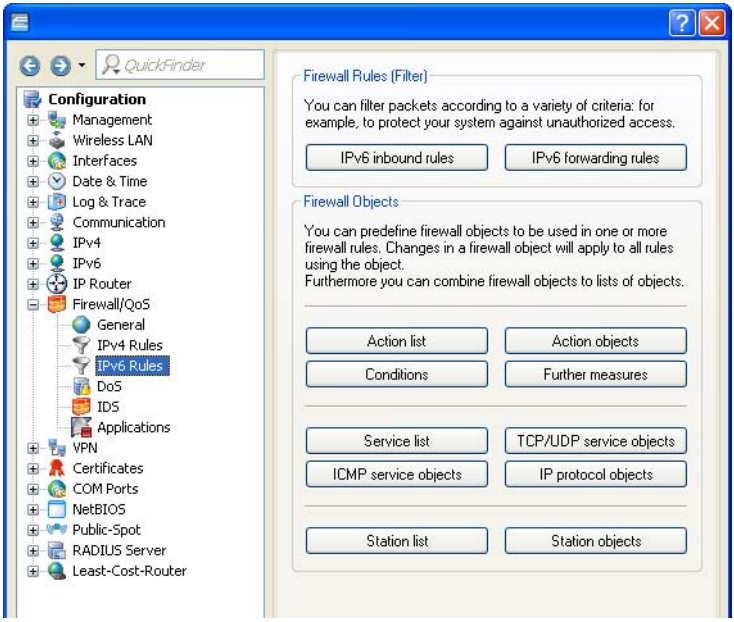
When the DNS server in your device receives a query about a station name, it responds with the IP address contained in the Host names list. For each station/host name you define either the IPv4 or the IPv6 address, or alternatively you can enter both IP addresses.

In LANconfig, the table with the station names and the associated IP addresses is under `IPv4:DNS:Host names`.



12.7.6 Configuring the IPv6 Firewall Rules

With LANconfig you can set the firewall rules under `Firewall/QoS:IPv6 Rules`.



The factory settings provide various objects and lists for the most important applications.

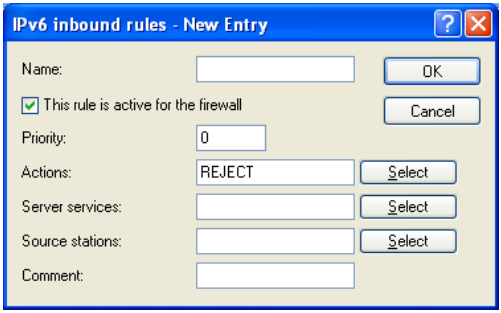
Hinweis: You cannot delete objects or lists if the firewall uses them in a forwarding or inbound rule.

IPv6 Inbound Rules

Using the „IPv6 inbound rules“ you set the rules that the IPv6 firewall should use to handle incoming traffic.

The factory settings provide various rules for the most important applications.

Click on „Add...“ to create a new rule.



You can set the following properties for the rule:

☐ „Name“

Specifies the name of the rule.

☐ „This rule is active for the firewall“

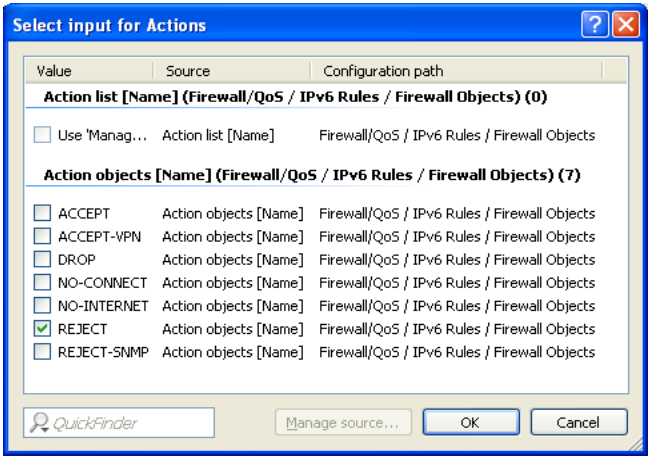
Enables the rule.

☐ „Priority“

Specifies the priority of the rule: The higher the value, the higher the priority.

☐ „Actions“

Specifies the action that the firewall performs if the rule condition is true. Using „Select“ you can choose one action or a list of actions.



If you make a new entry here, it initially appears under „Unknown source“. Next, highlight the entry for a source that you want to assign to the new entry, and click on „Manage source.“ Set the values for this entry, and save the new object. The new entry now appears as a new object in the list of the corresponding source.

☐ „Server services“

Determines the services which the firewall applies this rule to. Using „Select“ you can choose one service or a list of services.

☐ „Source stations“

Determines the source stations which the firewall applies this rule to. Using „Select“ you can choose a terminal device or a list of stations.

☐ „Comment“

Here you assign a meaningful description for the filter rule.

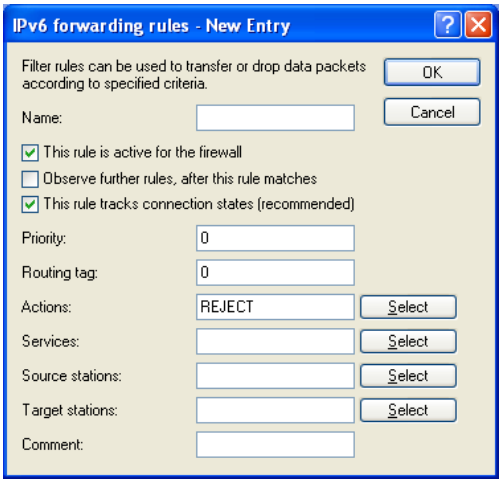
IPv6 Forwarding Rules

The „IPv6 forwarding rules“ button accesses dialog where you set the rules that the IPv6 firewall should use to handle forwarded traffic.

The factory settings provide various rules for the most important applications.

In order to change the order of the rules, highlight the specific rule in the table and move it up or down in the table by clicking on the arrow buttons. The firewall applies the rules one after the other from top to bottom.

Click on „Add...“ to create a new rule.



You can set the following properties for the rule:

☐ „Name“

Specifies the name of the rule.

☐ „This rule is active for the firewall“

Enables the rule.

☐ „Observe further rules after this rule matches“

If you enable this option, the firewall also applies the subsequent rules in the list. This is useful if the firewall should, for example, initially apply a group rule and then apply each rule to the individual objects in the group.

☐ „This rule tracks connection states (recommended)“

Select this option if the rule should track the TCP connection states.

☐ „Priority“

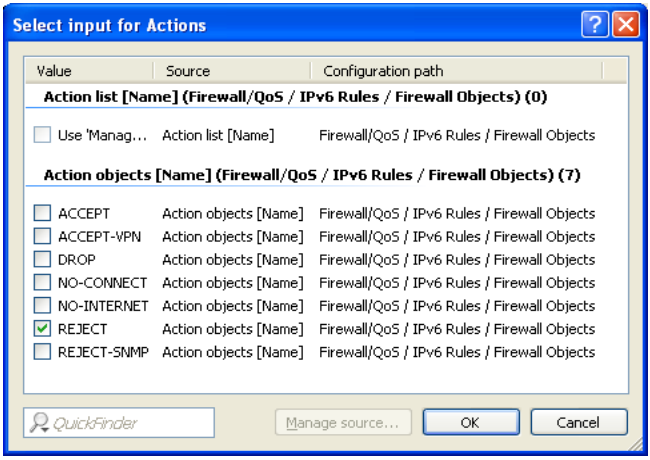
Specifies the priority of the rule: The higher the value, the higher the priority.

☐ „Routing tag“

The interface tag that you enter here is a value that uniquely identifies the network. All packets received by this device on this network will be internally marked with this tag. The interface tag makes it possible to separate the rules valid for this network.

☐ „Actions“

Specifies the action that the firewall performs if the rule condition is true. Using „Select“ you can choose one action or a list of actions.



If you make a new entry here, it initially appears under „Unknown source“. Next, highlight the entry for a source that you want to assign to the new entry, and click on „Manage source.“ Set the values for this entry, and save the new object. The new entry now appears as a new object in the list of the corresponding source.

☐ „Server services“

Determines the services which the firewall applies this rule to. Using „Select“ you can choose one service or a list of services.

☐ „Source stations“

Determines the source stations which the firewall applies this rule to. Using „Select“ you can choose a terminal device or a list of stations.

☐ „Target stations“

Determines the target stations which the firewall applies this rule to. Using „Select“ you can choose a terminal device or a list of stations.

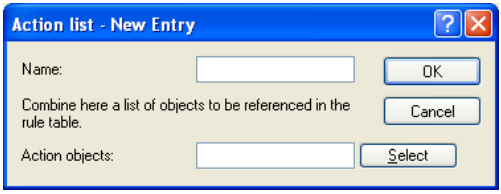
☐ „Comment“

Here you assign a meaningful description for the filter rule.

Action List

Using the „Action list“ button, you can collect actions into groups. The actions available here must first be defined using „Action objects“.

Click on „Add...“ to create a new rule.



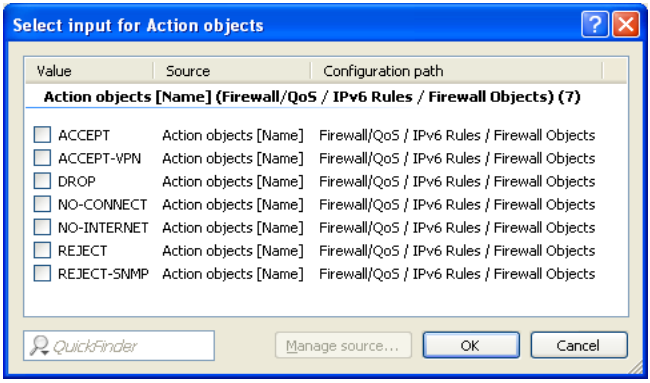
You can set the following properties for a list:

☐ „Name“

Determines the name of the list.

☐ „Action objects“

Determines the objects that you want to combine in this list. Using „Select“ you can choose one or more objects from a list.

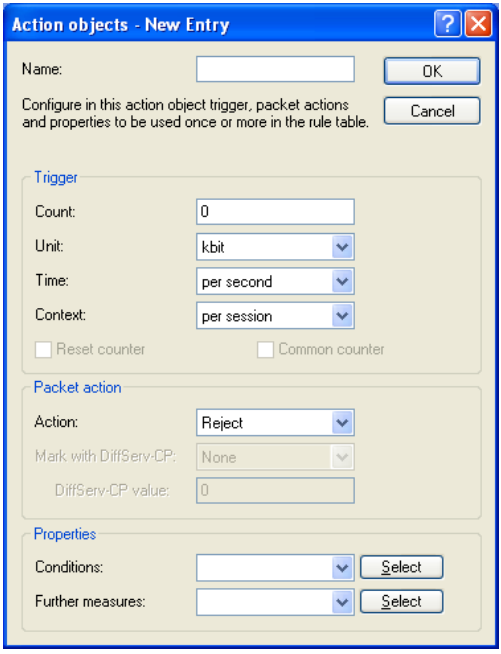

Select input for Action objects
Value
Source
Configuration path
Action objects [Name] (Firewall/QoS / IPv6 Rules / Firewall Objects) (7)
ACCEPT Action objects [Name] Firewall/QoS / IPv6 Rules / Firewall Objects
ACCEPT-VPN Action objects [Name] Firewall/QoS / IPv6 Rules / Firewall Objects
DROP Action objects [Name] Firewall/QoS / IPv6 Rules / Firewall Objects
NO-CONNECT Action objects [Name] Firewall/QoS / IPv6 Rules / Firewall Objects
NO-INTERNET Action objects [Name] Firewall/QoS / IPv6 Rules / Firewall Objects
REJECT Action objects [Name] Firewall/QoS / IPv6 Rules / Firewall Objects
REJECT-SNMP Action objects [Name] Firewall/QoS / IPv6 Rules / Firewall Objects
QuickFinder
Manage source...
OK
Cancel

If you make a new entry here, it initially appears under „Unknown source“. Next, highlight the entry for a source that you want to assign to the new entry, and click on „Manage source.“ Set the values for this entry, and save the new object. The new entry now appears as a new object in the list of the corresponding source.

Action Objects

Using the „Action objects“ button, you define actions that the IPv6 firewall runs when a filter is true.

Click on „Add...“ to create a new action.



You can set the following properties for the object:

☐ „Name“

Specifies the name of the object.

☐ „Count“

When this limit is exceeded, the firewall performs the action.

☐ „Unit“

Determines the unit for the limits. Select the corresponding value in the drop-down menu.

☐ „Time“

Determines the measurement period that the firewall applies to the limit. Select the corresponding value in the drop-down menu.

☐ „Context“

Determines the context that the firewall applies to the limit. Select the corresponding value in the drop-down menu.

☐ „Reset counter“

If you enable this option, the firewall resets the counter after running the action.

Hinweis: You can only activate this option if you selected "absolute" in the „time“ value.

☐ „Common counter“

If you enable this option, the firewall adds all action triggers together in one counter.

Hinweis: You can only activate this option if you selected "per station" or "global" in the „Context“ value.

☐ „Action“

Determines the action the firewall performs when the limit is reached.

The following options are possible:

- **Reject**: The firewall rejects the data packet and sends an appropriate notification to the sender.
- **Drop**: The firewall discards the data packet without notification.
- **Transmit**: The firewall accepts the data packet.

☐ „Mark with DiffServ-CP“

Determines the priority of the data packets (differentiated services, DiffServ), with which the firewall should transfer the data packets.

Hinweis: You can only activate this option if you selected "transmit" in the „Action“ value.

Hinweis: Further information about DiffServ CodePoints is available in the Reference Manual under the section "QoS".

☐ „DiffServ-CP value“

Sets the value for the differentiated services code point (DSCP).

Hinweis: You can only activate this option if you selected "Value" in „Mark with DiffServ-CP“.

☐ „Conditions“

Determines which conditions must be met in order for the action to be performed. The item „Conditions“ is used to specify any conditions.

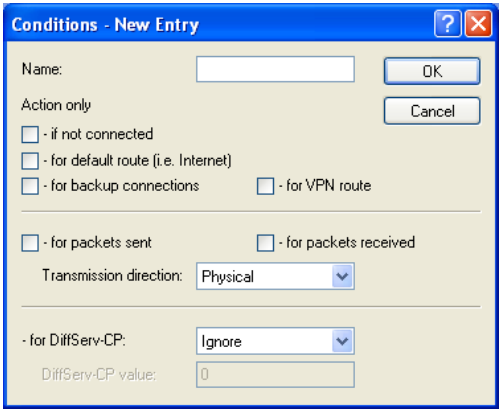
☐ „Further measures“

Determines which trigger actions the firewall should start in addition to filtering the data packets. You can specify trigger actions under the „Further measures“.

Conditions

Use the „Conditions“ button to specify the conditions that have to be met for the forwarding and inbound rules to apply.

Click on „Add...“ to create a new condition.



You can set the following properties for the condition:

☐ „Name“

Specifies the name of the object.

☐ „Action only – if not connected“

Select this option if the firewall should only perform the action if there is no data connection.

☐ „Action only – for default route (e.g. Internet)“

Select this option if the firewall should only perform the action if there is a data connection over the default route.

☐ „Action only – for backup connections“

Select this option if the firewall should only perform the action if the connection is a backup connection.

☐ „Action only – for VPN route“

Select this option if the firewall should only perform the action if the connection is a VPN connection.

☐ „Action only – for packets sent“

Select this option if the firewall should only perform the action for packets sent.

☐ „Action only – for packets received“

Select this option if the firewall should only perform the action for packets received.

☐ „Transmission direction“

Determines whether the transport direction refers to the logical connection or the physical data transmission over the respective interface.

☐ „Action only – for DiffServ-CP“

Determines the priority that the data packets (differentiated services, DiffServ) have to have, so that the condition is met.

Hinweis: Further information about DiffServ CodePoints is available in the Reference Manual under the section "QoS".

☐ „DiffServ-CP value“

Determines the value for the Differentiated Services Code Point (DSCP).

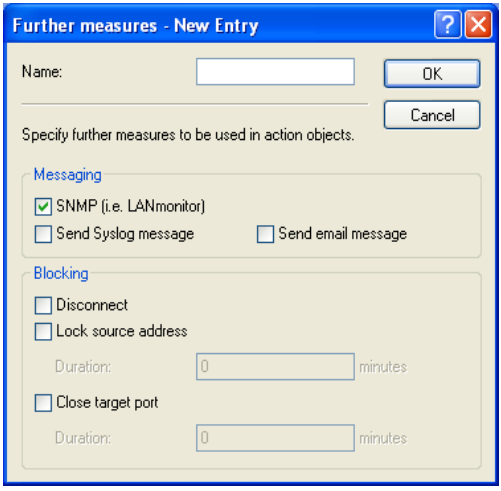
Enter a value here if you selected the "Value" option in the „– for DiffServ-CP“ field.

Hinweis: Further information about DiffServ CodePoints is available in the Reference Manual under the section "QoS".

Further Measures

Use the „Further measures“ button to define further measures that the firewall performs after you apply the forwarding and inbound rules.

Click on „Add...“ to create a new measure.



You can set the following properties for the trigger actions:

☐ „Name“

Specifies the name of the object.

☐ „SNMP (e.g. LANmonitor)“

Select this option if the firewall should send a notification via SNMP. You can receive this notification, e.g., with LANmonitor.

☐ „Send SYSLOG message“

Select this option if the firewall should send a SYSLOG notification via SNMP.

Hinweis: For more information about SYSLOG, refer to the chapter "Diagnostics" in the section "SYSLOG" in the Reference Guide.

☐ „Send e-mail message“

Select this option, if the firewall should send a notification by e-mail.

Hinweis: If you want to receive e-mail notifications, you must enter an e-mail address in `Firewall/QoS.General.Administrator e-mail`.

☐ „Disconnect“

Select this option if the firewall should disconnect.

☐ „Lock source address“

Select this option if the firewall should block the source address. The firewall registers the blocked IP address, the lockout period, as well as the underlying rule in the „Host-block-list“ under `Status:IPv6:Firewall`.

☐ „Duration“

If the firewall should block the sender, you can set the duration of the lock in minutes. The value "0" disables the lock because, in practice, the lockout period expires after 0 minutes.

☐ „Close target port“

Select this option, if the firewall should block the target port. The firewall registers the blocked destination IP address, the protocol, the destination port, the lockout period, as well as the underlying rule in the „Port-block-list“ under `Status:IPv6:Firewall`.

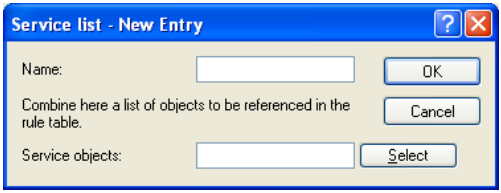
☐ „Duration“

If the firewall should block the target port, you can set the duration of the lock in minutes. The value "0" disables the lock because, in practice, the lockout period expires after 0 minutes.

Service List

Using the „Service list“ button, you can collect services into groups. You first define the services under „TCP/UDP service objects“, „ICMP service objects“ and „IP protocol objects“.

Click on „Add...“ to specify a new service.



You can set the following properties for a list:

☐ „Name“

Determines the name of the list.

☐ „Service objects“

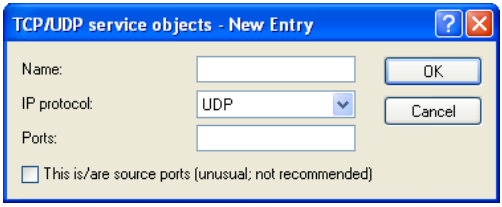
Determines the objects that you want to combine in this list. Using „Select“ you can choose one or more objects from a list.

If you make a new entry here, it initially appears under „Unknown source“. Next, highlight the entry for a source that you want to assign to the new entry, and click on „Manage source.“ Set the values for this entry, and save the new object. The new entry now appears as a new object in the list of the corresponding source.

TCP/UDP Service Objects

Using the „TCP/UDP service objects“ button, you define TCP/UDP services that the IPv6 firewall can use in filter rules.

Click on „Add...“ to create a new service.



You can set the following properties for the rule:

☐ „Name“

Specifies the name of the object.

☐ „IP protocol“

Specifies the protocol of the service

☐ „Ports“

Specifies the ports for the service. Separate multiple ports with a comma.

Hinweis: Lists with the official protocol and port numbers are available in the Internet at www.iana.org.

☐ „This is/are source ports“

Determines whether the specified ports are source ports.

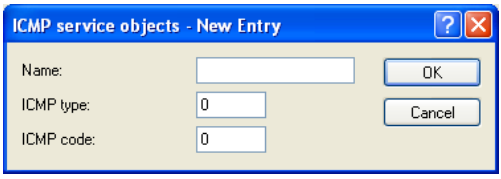
Hinweis: In certain scenarios, it may be useful to specify a source port. This is unusual. Selecting "No" is recommended.

ICMP Service Objects

Using the „ICMP service objects“ button, you define ICMP services that the IPv6 firewall can use in filter rules.

Hinweis: Lists with the official ICMP types and port codes are available in the Internet under www.iana.org.

Click on „Add...“ to create a new service.



You can set the following properties for the rule:

☐ „Name“

Specifies the name of the object.

☐ „ICMP type“

Specifies the type of the ICMP service.

☐ „ICMP code“

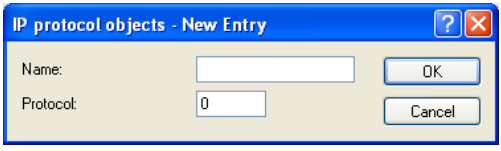
Specifies the code of the ICMP service.

IP Protocol Objects

Using the „IP protocol objects“ button, you define IP protocol objects that the IPv6 firewall can use in filter rules.

Hinweis: Lists with the official protocol and port numbers are available in the Internet at www.iana.org.

Click on „Add...“ to create a new object.



You can set the following properties for the rule:

☐ „Name“

Specifies the name of the object.

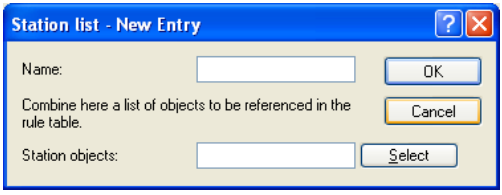
☐ „Protocol“

Defines the protocol number.

Station List

Using the „Station list“ button, you can collect stations into groups. The terminal devices must previously be defined using „Station objects“.

Click on „Add...“ to create a new list.



You can set the following properties for a list:

☐ „Name“

Determines the name of the list.

☐ „Station objects“

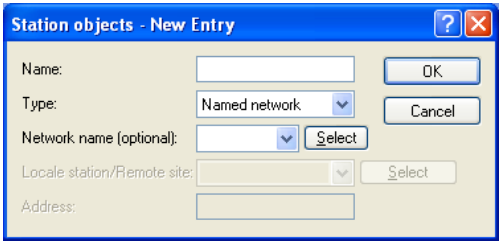
Determines the objects that you want to combine in this list. Using „Select“ you can choose one or more objects from a list.

If you make a new entry here, it initially appears under „Unknown source“. Next, highlight the entry for a source that you want to assign to the new entry, and click on „Manage source.“ Set the values for this entry, and save the new object. The new entry now appears as a new object in the list of the corresponding source.

Station Objects

Using the „Station objects“ button, you define the terminal devices that the IPv6 firewall can use in filter rules.

Click on „Add...“ to create a new object.



You can set the following properties for the object:

☐ „Name“

Specifies the name of the object.

☐ „Type“

Determines the station type.

☐ „Network name“

Here you enter the name of the network if you selected the appropriate option in the „Type“ field.

Hinweis: Entering the network name is optional.

☐ „Remote site“

Here you enter the name of the remote site if you selected the appropriate option in the „Type“ field.

☐ „Address“

Here you enter the address of the remote site if you selected the appropriate option in the „Type“ field.

12.8 Tutorials

12.8.1 Setting up IPv6 Internet Access

You can set up access to an IPv6 network if

- You have an IPv6-capable device,
- You use a tunneling technology and
- Your provider supports a native IPv6 network or you have access to a so-called tunnel broker who can mediate your IPv6 packets.

IPv6 Access Using the Setup Wizard in LANconfig

The Setup Wizard assists you with the configuration of IPv6 access with your equipment.

The Wizard presents following options:

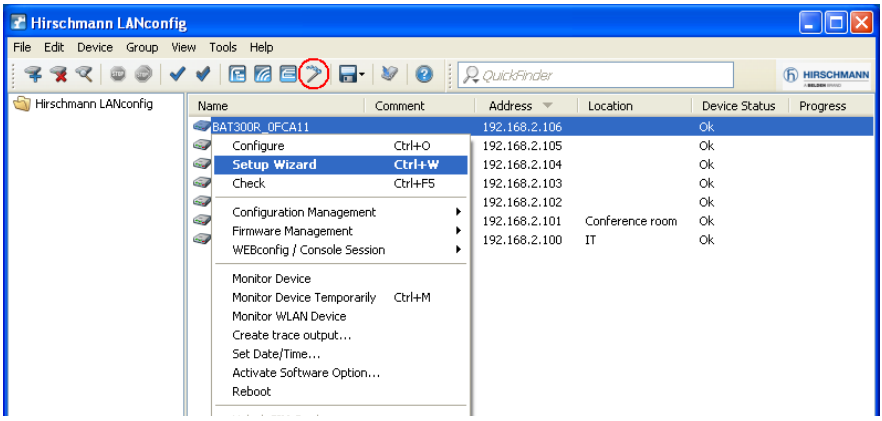
- `Set up IPv6 access for a new, unconfigured device.`
- `Set up IPv6 access in addition to a functioning IPv4 access for an existing device.`

Setup Wizard – Setting up IPv6 in a New Device

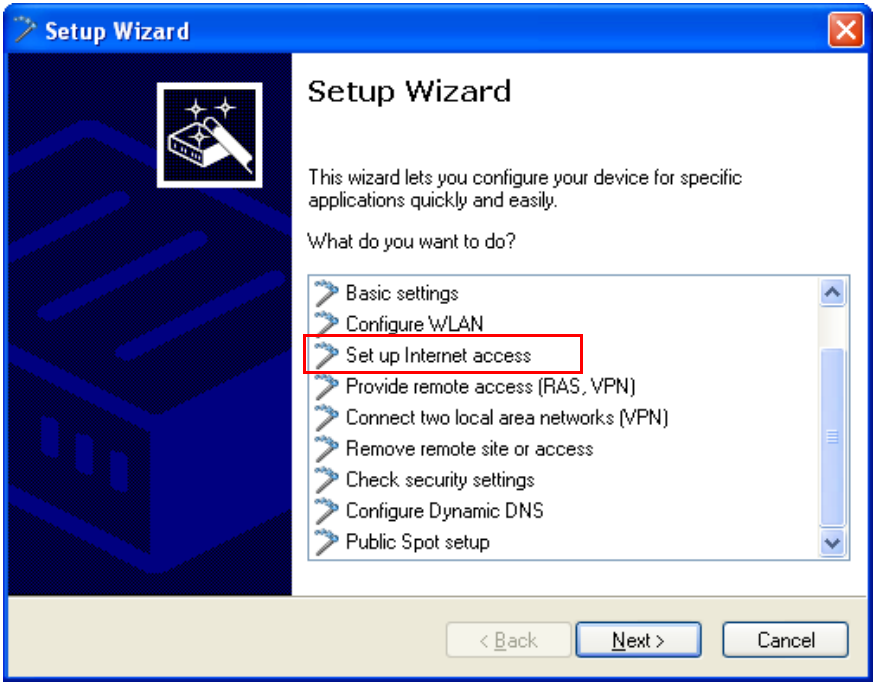
If you have connected up a new device but not have yet configured it, you have the option of using a Setup Wizard to set up IPv4 and IPv6 connections.

To save your entries and proceed to the next screen, click „Next“.

☐ Then start the Setup Wizard in LANconfig. Highlight the device to be configured. The Setup Wizard is started either by right-clicking and using the context menu, or with the Magic Wand icon in the toolbar.



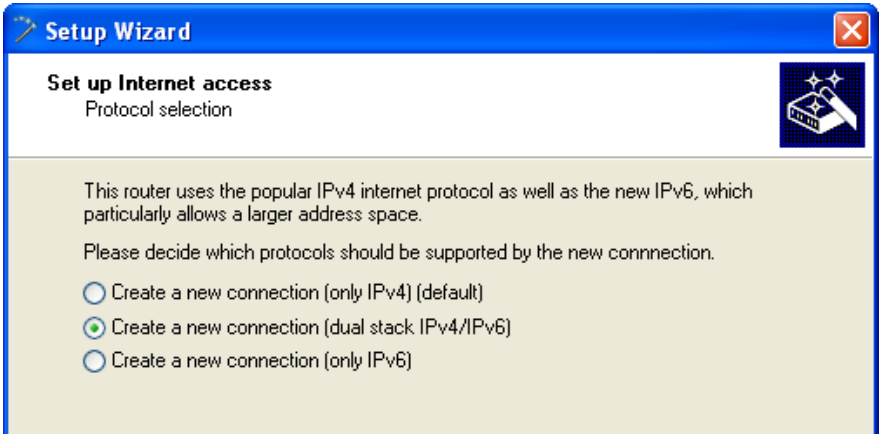
☐ In the Setup Wizard, select the option „Set up Internet access“.


Setup Wizard
Setup Wizard
This wizard lets you configure your device for specific applications quickly and easily.
What do you want to do?
Basic settings
Configure WLAN
Set up Internet access
Provide remote access (RAS, VPN)
Connect two local area networks (VPN)
Remove remote site or access
Check security settings
Configure Dynamic DNS
Public Spot setup
< Back
Next >
Cancel

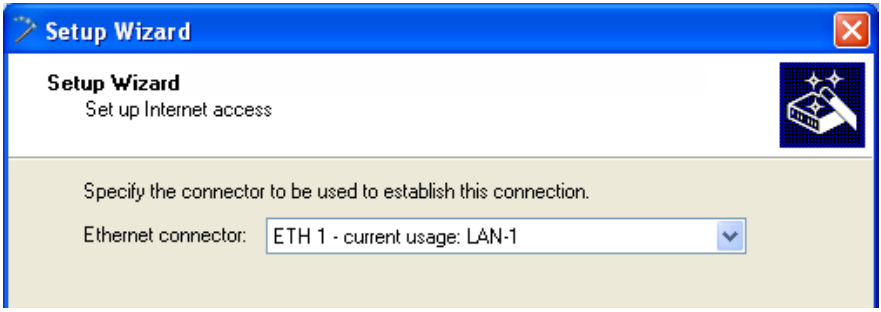
☐ You can choose from the following options:

- Set up a dual-stack connection. This is IPv4-and IPv6-capable and currently the recommended option for a new device.
- Set up an IPv4-only connection.
- Set up an IPv6-only connection.

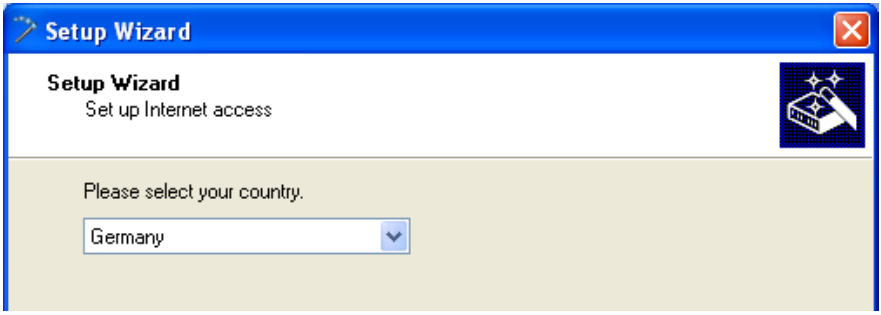
In the following we take you through the setup of a dual-stack connection. Activate the appropriate selection.


Setup Wizard
Set up Internet access
Protocol selection
This router uses the popular IPv4 internet protocol as well as the new IPv6, which particularly allows a larger address space.
Please decide which protocols should be supported by the new connnection.
Create a new connection (only IPv4) (default)
Create a new connection (dual stack IPv4/IPv6)
Create a new connection (only IPv6)

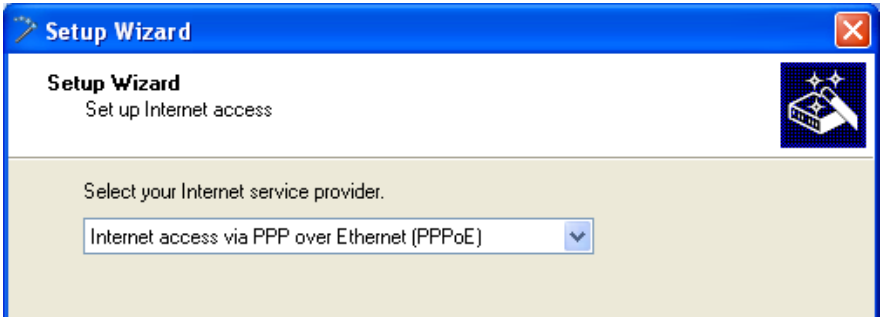
☐ Set the interface to be used for the connection.


Setup Wizard
Setup Wizard
Set up Internet access
Specify the connector to be used to establish this connection.
Ethernet connector:
ETH 1 - current usage: LAN-1

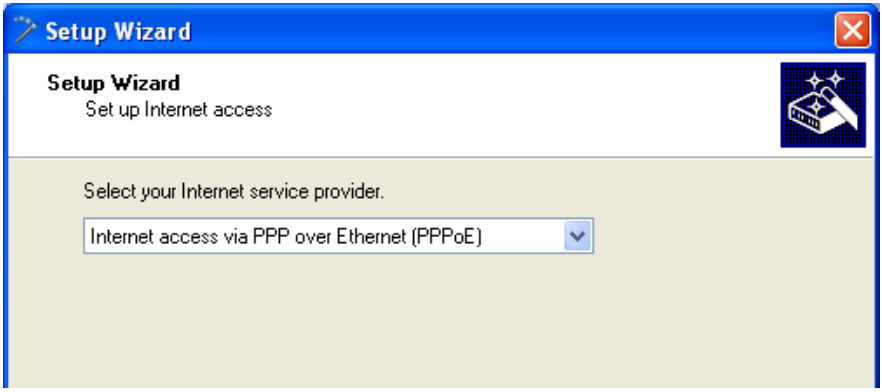
☐ Select your country from the list.



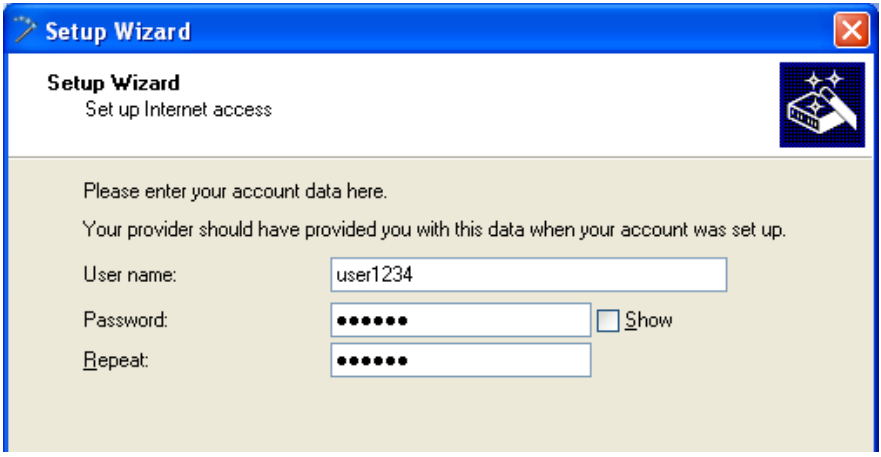
☐ Select your Internet provider.


Setup Wizard
Setup Wizard
Set up Internet access
Select your Internet service provider.
Internet access via PPP over Ethernet (PPPoE)

☐ Enter a name for this data connection.

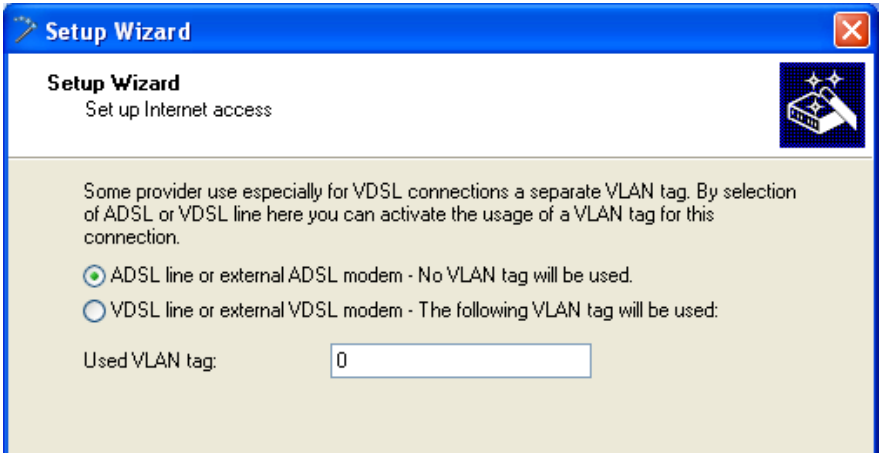

Setup Wizard
Setup Wizard
Set up Internet access
Select your Internet service provider.
Internet access via PPP over Ethernet (PPPoE)

☐ Enter the login details given to you by your provider for setting up your Internet access.



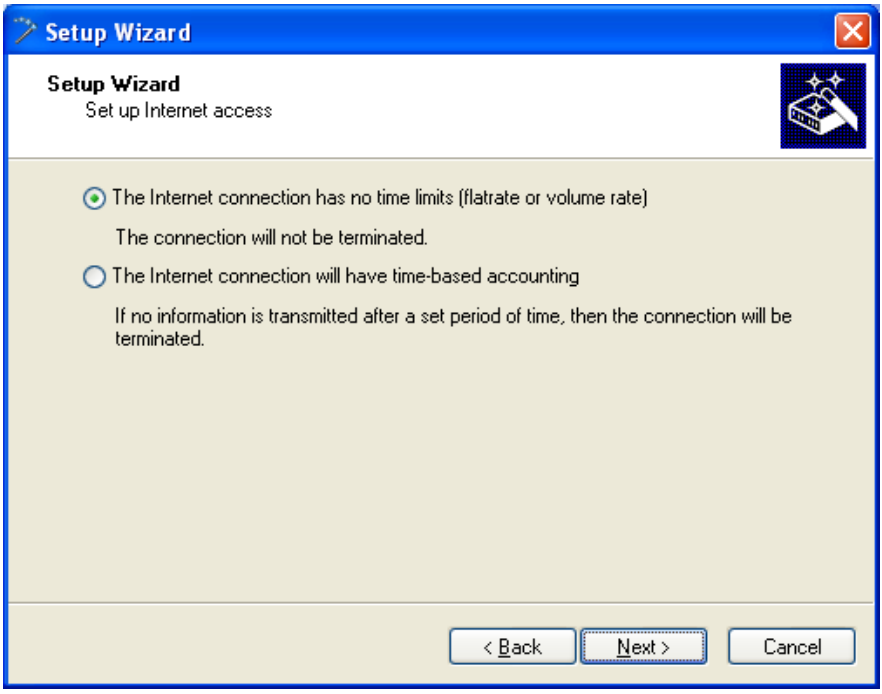
Hinweis: Depending on the provider, the type and number of fields may vary.

☐ If you use PPPoE: Specify what kind of DSL connection you have and which particular VLAN tag your provider uses.


Setup Wizard
Setup Wizard
Set up Internet access
Some provider use especially for VDSL connections a separate VLAN tag. By selection of ADSL or VDSL line here you can activate the usage of a VLAN tag for this connection.
ADSL line or external ADSL modem - No VLAN tag will be used.
VDSL line or external VDSL modem - The following VLAN tag will be used:
Used VLAN tag:
0

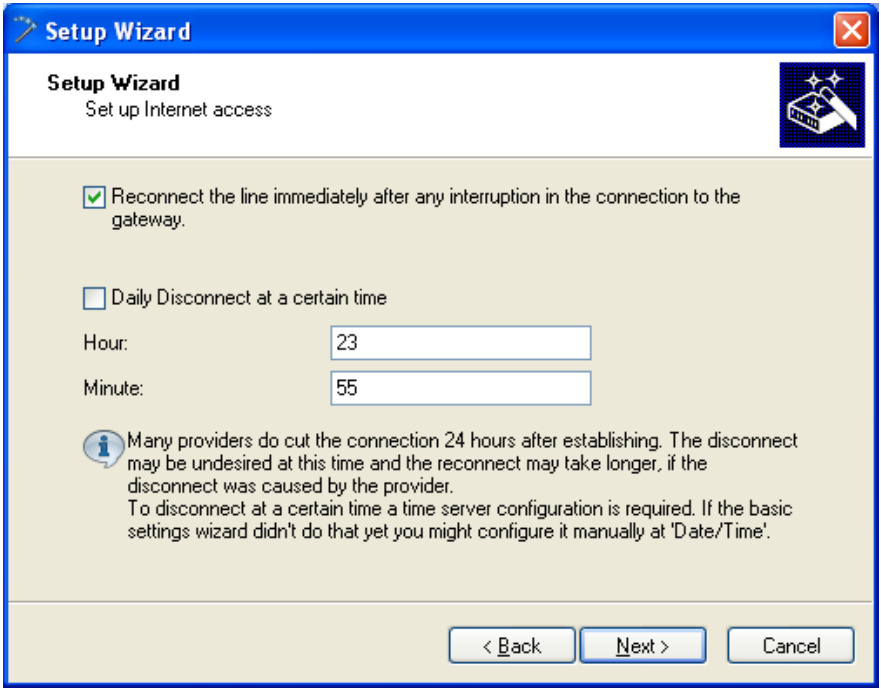
Hinweis: Depending on the provider, the type and number of fields may vary.

☐ If you use PPPoE: Specify whether your Internet connection is subject to a data flat rate, a data quota, or if your provider charges your Internet access based on time.

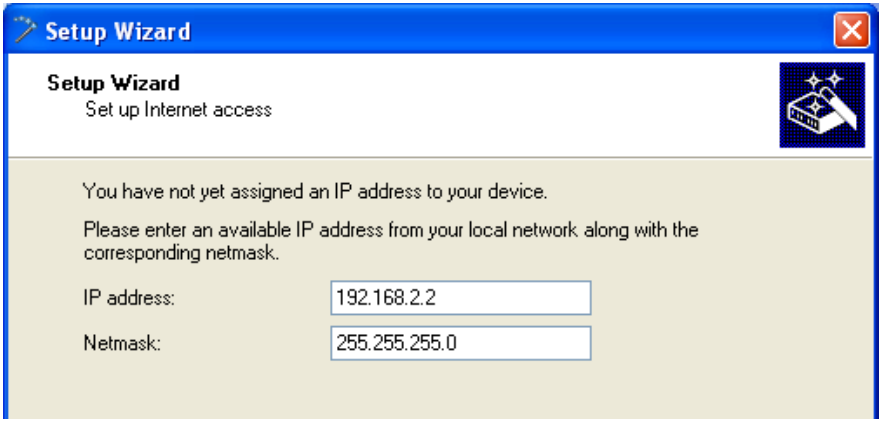

Setup Wizard
Setup Wizard
Set up Internet access
The Internet connection has no time limits (flatrate or volume rate)
The connection will not be terminated.
The Internet connection will have time-based accounting
If no information is transmitted after a set period of time, then the connection will be terminated.
< Back
Next >
Cancel

Hinweis: Depending on the provider, the type and number of fields may vary.

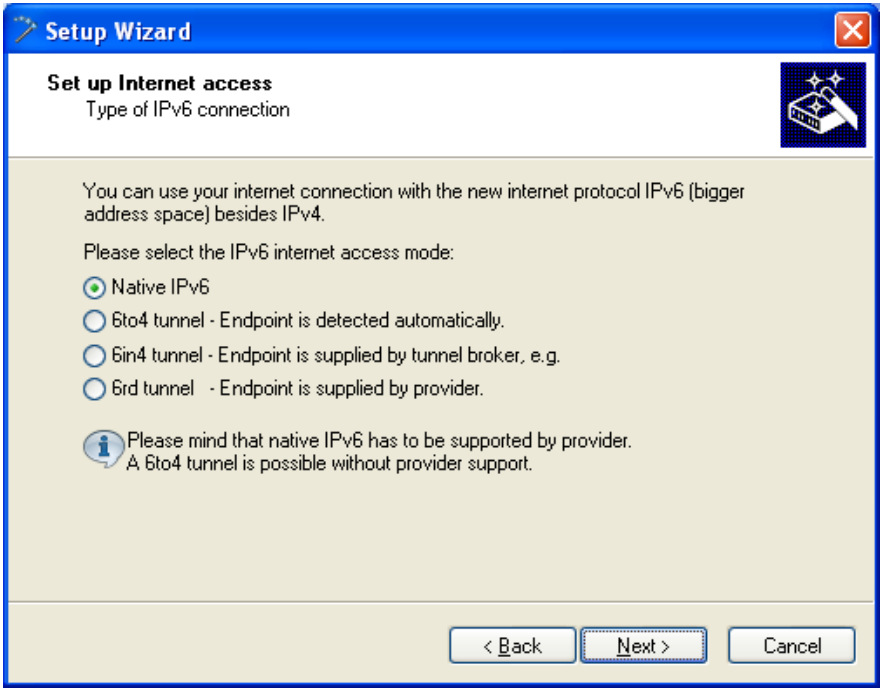
☐ Specify how you want the device to behave in case of disconnection. You can also specify if and when the device is to carry out a forced re-connection.


Setup Wizard
Setup Wizard
Set up Internet access
Reconnect the line immediately after any interruption in the connection to the gateway.
Daily Disconnect at a certain time
Hour:
23
Minute:
55
Many providers do cut the connection 24 hours after establishing. The disconnect may be undesired at this time and the reconnect may take longer, if the disconnect was caused by the provider.
To disconnect at a certain time a time server configuration is required. If the basic settings wizard didn't do that yet you might configure it manually at 'Date/Time'.
< Back
Next >
Cancel

☐ If your device does not yet have an IP address, enter a new IP address and corresponding netmask.


Setup Wizard
Setup Wizard
Set up Internet access
You have not yet assigned an IP address to your device.
Please enter an available IP address from your local network along with the corresponding netmask.
IP address:
192.168.2.2
Netmask:
255.255.255.0

☐ Select the type of IPv6 Internet access.

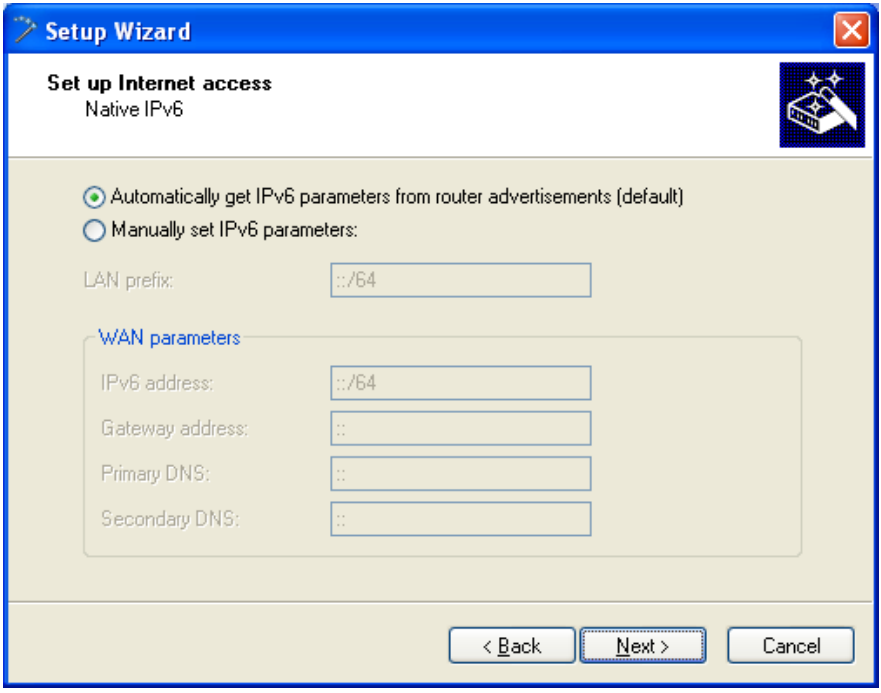

Setup Wizard
Set up Internet access
Type of IPv6 connection
You can use your internet connection with the new internet protocol IPv6 (bigger address space) besides IPv4.
Please select the IPv6 internet access mode:
Native IPv6
6to4 tunnel - Endpoint is detected automatically.
6in4 tunnel - Endpoint is supplied by tunnel broker, e.g.
6rd tunnel - Endpoint is supplied by provider.
Please mind that native IPv6 has to be supported by provider.
A 6to4 tunnel is possible without provider support.
< Back
Next >
Cancel

You can select from the following options:

- „Additional native IPv6“: Configure a direct data connection without a tunnel.
- „6to4 tunnel“: Start the wizard to configure a 6to4 tunnel.
- „6in4 tunnel“: Use the input mask to set the parameters for the 6in4 tunnel.
- „6rd tunnel“: Use the input mask to set the parameters for the 6rd tunnel.

Select the option for setting up a native IPv6 Internet connection.

☐ Accept the default setting of „Automatically take IPv6 parameters from router advertisements.“



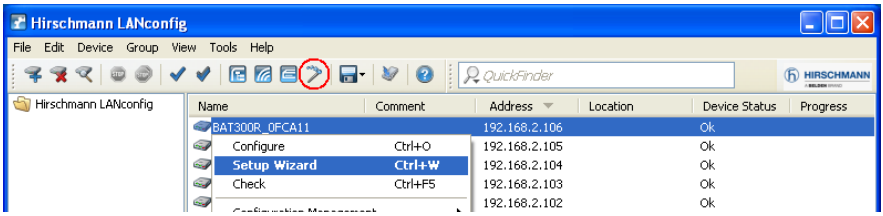
☐ You have completed the setup of the native IPv6 Internet access. Click on „Finish“ when you are done and the wizard will save your entries to the device.

Setup Wizard – Setting up IPv6 on an Existing Device

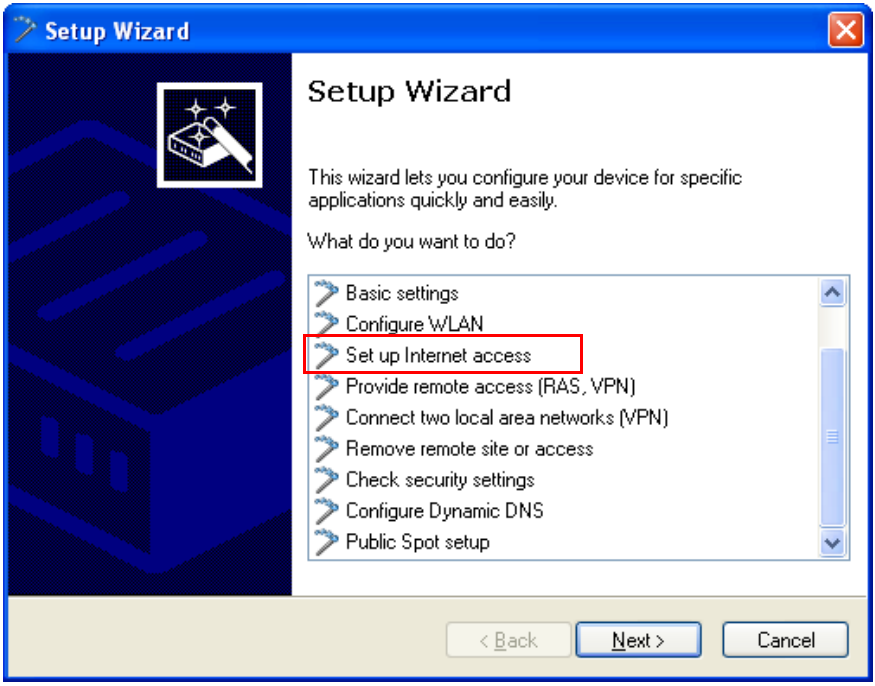
If you have a device configured for IPv4 and you wish to set up an additional IPv6 connection, you have the option of setting up the IPv6 connections with the Setup Wizard.

To save your entries and proceed to the next screen, click „Next“.

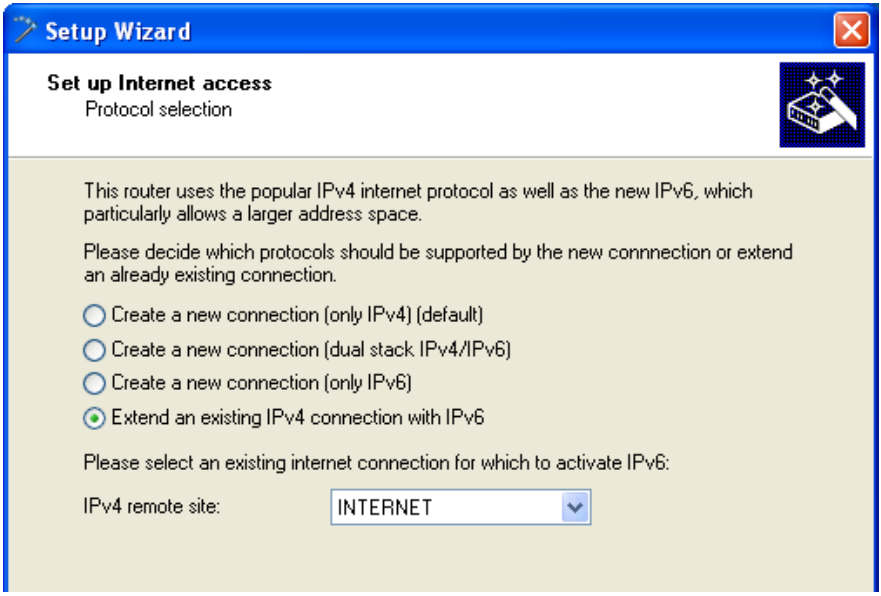
☐ Then start the Setup Wizard in LANconfig. Highlight the device to be configured. The Setup Wizard is started either by right-clicking and using the context menu, or with the Magic Wand icon in the toolbar



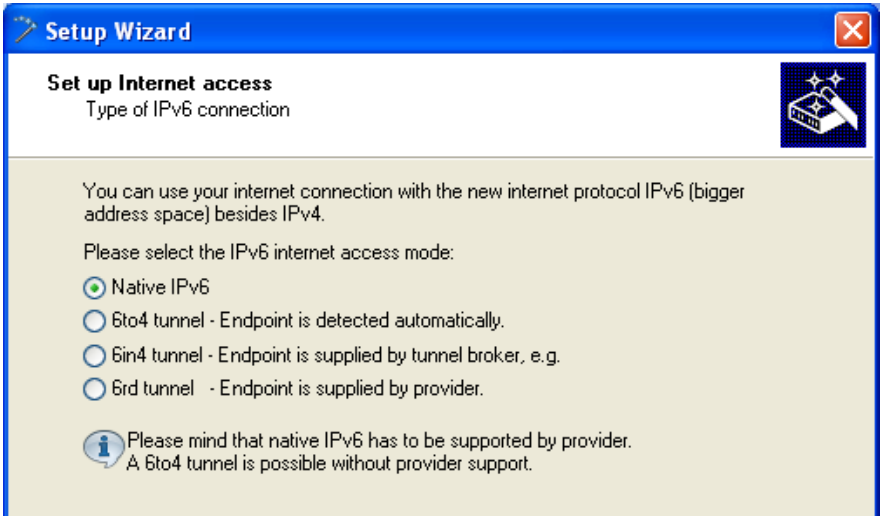
☐ In the Setup Wizard, select the option „Set up Internet access“. To continue, click on „Next“.


Setup Wizard
Setup Wizard
This wizard lets you configure your device for specific applications quickly and easily.
What do you want to do?
Basic settings
Configure WLAN
Set up Internet access
Provide remote access (RAS, VPN)
Connect two local area networks (VPN)
Remove remote site or access
Check security settings
Configure Dynamic DNS
Public Spot setup
< Back
Next >
Cancel

☐ Because your device is already IPv4-capable, the Setup Wizard gives you the opportunity to extend your existing settings with IPv6. Select this option and click on „Next.“


Setup Wizard
Set up Internet access
Protocol selection
This router uses the popular IPv4 internet protocol as well as the new IPv6, which particularly allows a larger address space.
Please decide which protocols should be supported by the new connnection or extend an already existing connection.
Create a new connection (only IPv4) (default)
Create a new connection (dual stack IPv4/IPv6)
Create a new connection (only IPv6)
Extend an existing IPv4 connection with IPv6
Please select an existing internet connection for which to activate IPv6:
IPv4 remote site:
INTERNET

☐ Select the type of IPv6 Internet access.

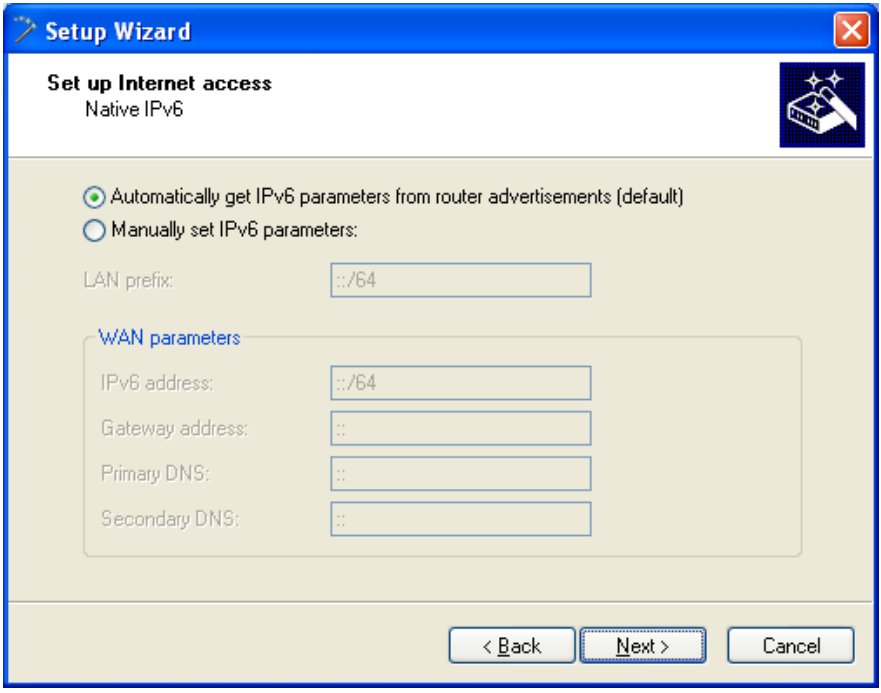

Setup Wizard
Set up Internet access
Type of IPv6 connection
You can use your internet connection with the new internet protocol IPv6 (bigger address space) besides IPv4.
Please select the IPv6 internet access mode:
Native IPv6
6to4 tunnel - Endpoint is detected automatically.
6in4 tunnel - Endpoint is supplied by tunnel broker, e.g.
6rd tunnel - Endpoint is supplied by provider.
Please mind that native IPv6 has to be supported by provider.
A 6to4 tunnel is possible without provider support.

You can select from the following options:

- „Additional native IPv6“: Configure a direct data connection without a tunnel.
- „6to4 tunnel“: Start the wizard to configure a 6to4 tunnel.
- „6in4 tunnel“: Use the input mask to set the parameters for the 6in4 tunnel.
- „6rd tunnel“: Use the input mask to set the parameters for the 6rd tunnel.

Select the option for setting up a native IPv6 Internet connection.

☐ Accept the default setting of „Automatically take IPv6 parameters from router advertisements.“



☐ You have completed the setup of the native IPv6 Internet access. Click on „Finish“ when you are done and the wizard will save your entries to the device.

12.8.2 Setting up a 6to4 Tunnel

The use of a 6to4 tunnel is feasible when

- Your device is IPv6 capable and you want to access IPv6 services,
- Your provider does not support a native IPv6 network and
- You do not have access to a so-called tunnel broker who can mediate your IPv6 packets.

When using a 6to4 tunnel, the lack of support of IPv6 by the provider means the device does not receive an IPv6 address or an IPv6 prefix.

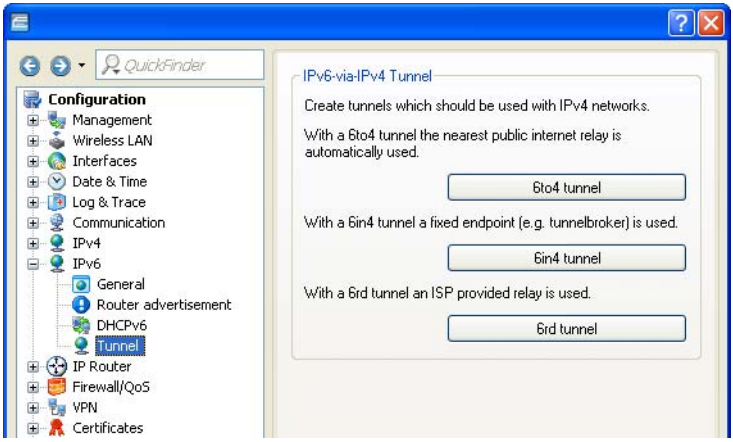
The device calculates its own unique prefix from "2002::/16" and the hexadecimal representation of its own public IPv4 address from the provider. This application only works if the device has a public IPv4 address. The device does not receive a public IPv4 address but an IPv4 address from a private address range only, for example when it accesses the Internet via UMTS and the provider supplies an IP address from its private address range, or if the device does not access the Internet directly, but is "behind" another router.

Hinweis: Connections through a 6to4 tunnel work with relays that are selected by the IPv4 Internet provider's backbone. The device administrator has no influence on relay selection. Furthermore, the relay used can change without the administrator knowing about it. For this reason, data connections via a 6to4 tunnels are suitable **for test purposes only**. In particular, avoid using 6to4-tunnel data connections for productive systems or for the transmission of confidential data.

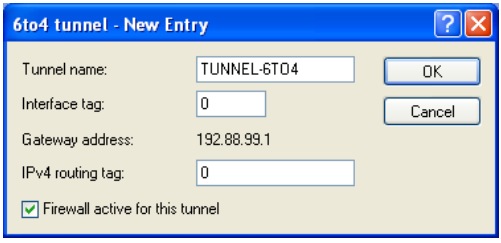
Working with LANconfig

To set up a 6to4 tunnel with LANconfig, proceed as follows:

- ☐ Start LANconfig. LANconfig now automatically searches the local network for devices.
- ☐ Select the device on which you want to set up a 6to4 tunnel. Select it with a left-click and start the configuration from the menu bar with `Device:Configure`.
- ☐ Navigate to `IPv6:Tunnel` and click on „6to4 tunnel“.



☐ Click on „Add“ to create a new 6to4 tunnel.



☐ Set the name of the 6to4 tunnel.

☐ Set the „Interface tag“ to a value that uniquely identifies the network. All packets received by this device on this network will be internally marked with this tag. The interface tag enables the routes which are valid for this network to be separated even without explicit firewall rules.

☐ The „Gateway address“ is set by default to the anycast address "192.88.99.1". This address can only be changed with WEBconfig or Telnet.

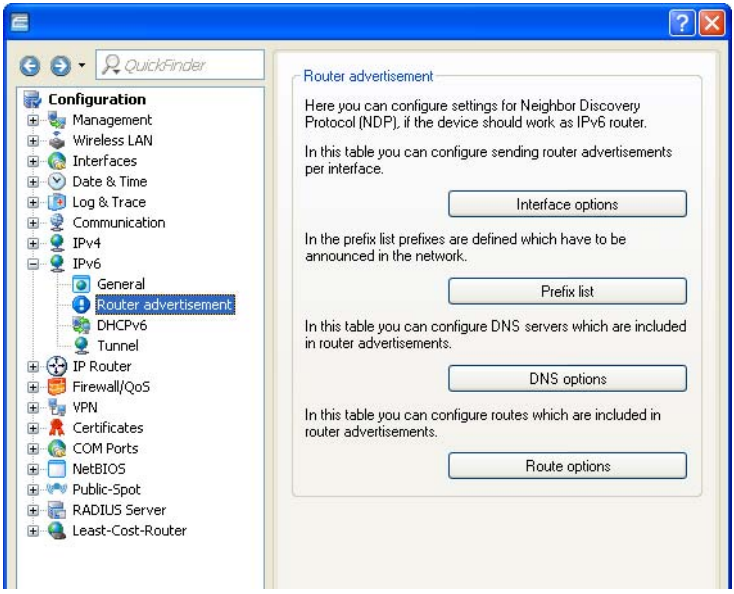
☐ Here you define the routing tag that the device uses to determine the route to the associated remote gateway. The „IPv4 routing tag“ specifies which tagged IPv4 route is to be used for the data packets to reach their destination address.

☐ The default value is this tunnel's firewall.

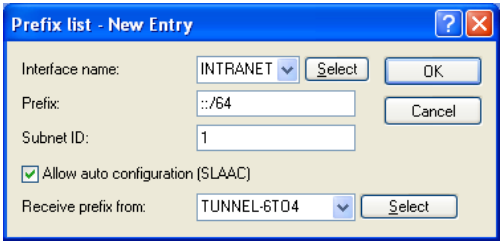
Hinweis: If you disable the global firewall, you should also disable the firewall for the tunnel.

☐ Accept your entries with „OK“.

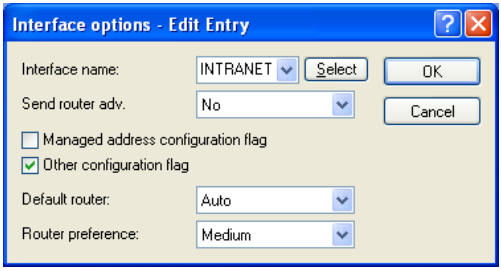
☐ Change to the directory `IPv6:Router advertisements`.



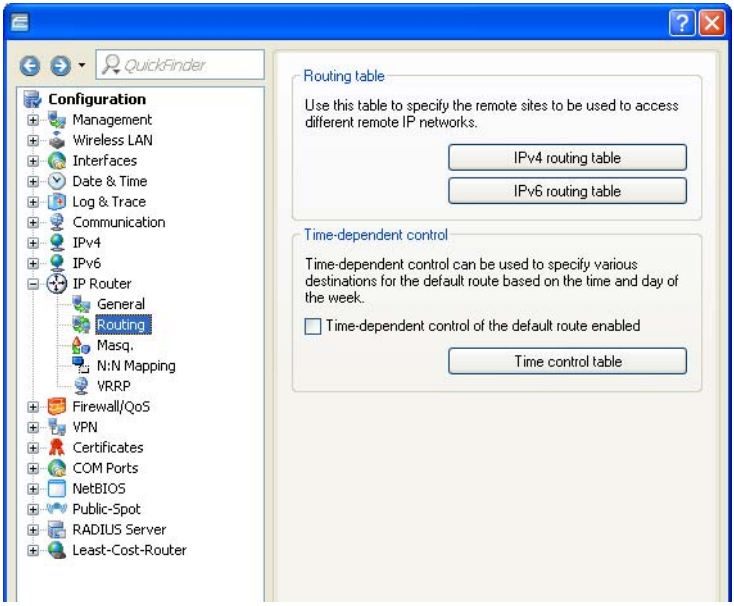
☐ Open the „Prefix list“ and click on „Add.“



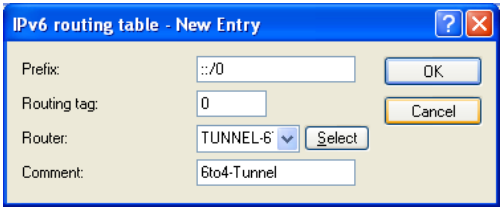
- ☐ Enter a name for the interface that is used by the 6to4 tunnel, e.g. "INTRANET".
- ☐ Set the value for the „Prefix“ to "::/64" in order to accept the prefix issued by the provider automatically and in its entirety.
- ☐ Accept the default value of "1" for the „Subnet ID“.
- ☐ Accept the activated option „Stateless address configuration“.
- ☐ In the field „Prefix delegation from“, enter the name of the tunnel that you have defined earlier, e.g. in the example above "TUNNEL-6TO4".
- ☐ Accept your entries with „OK“.
- ☐ In the directory `IPv6:Router advertisements`, open the „Interface options“, select the entry INTRANET and click on „Edit“.
- ☐ In the drop-down menu „Send router advertisements“ select the option 'Yes'.



- ☐ Accept all other default values ??without change.
- ☐ Save your entries with „OK“.
- ☐ Change to the directory `IP router:Routing`.



☐ Open the „IPv6 routing table“ and click on „Add“.



☐ Set the „Prefix“ to the value "::/0".

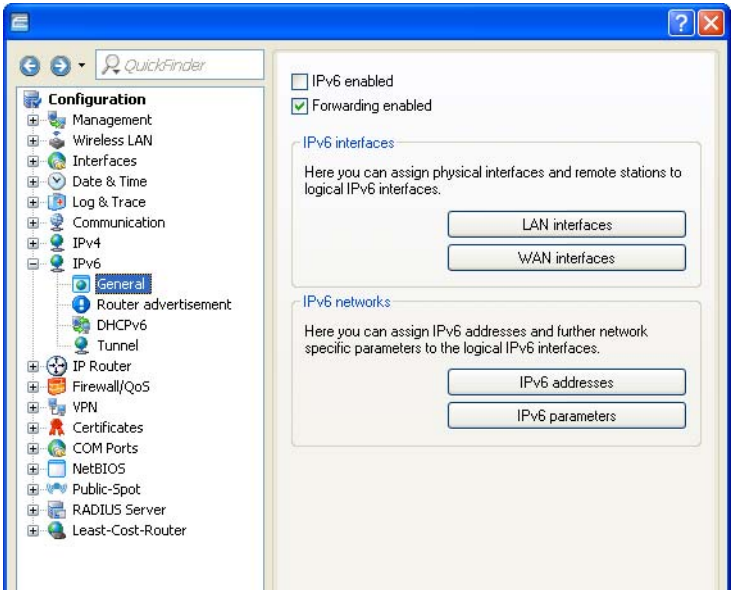
☐ In the field „Routing tag“ accept the default value "0".

☐ In the field „Router“, select from the list the name of the tunnel that you defined earlier, e.g. in the example above "TUNNEL-6TO4".

☐ Enter a descriptive „Comment “for this entry.

☐ Save your entries with „OK“.

☐ Change to the directory `IPv6:General` and enable the IPv6 stack.

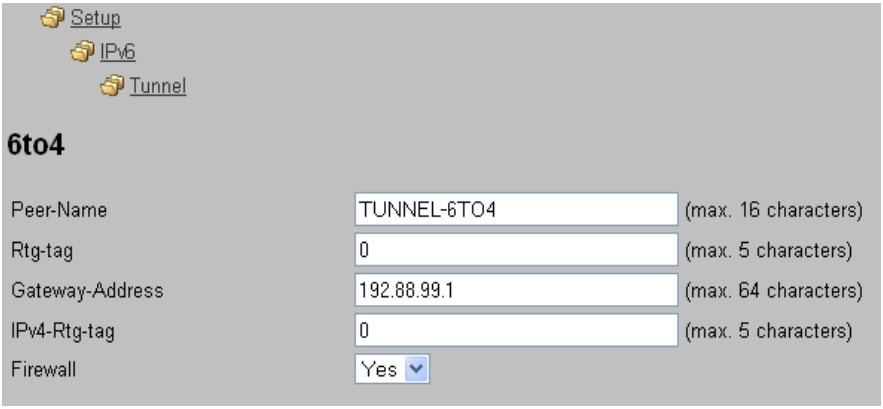


Working with WEBconfig

To set up a 6to4 tunnel with WEBconfig, proceed as follows:

☐ Type into your browser's address bar the address of the device to be set up with a 6to4 tunnel.

☐ Change to the directory `HiLCOS Menu Tree:Setup:IPv6:Tunnel:6to4` and click „Add“.



☐ Enter a name for the remote peer, e.g. "TUNNEL-6TO4".

☐ Leave the „Routing tag“ unchanged as the default value "0".

☐ As the „Gateway address“ you can accept the default value "192.88.99.1". This is the default anycast address for 6to4 relays that your device connects to.

Hinweis: This address is the reason why a 6to4 tunnel is unstable and susceptible to interception by unauthorized users. There is no assurance that a 6to4 relay will be available, and publicly available 6to4 relays may not be trustworthy. There is no certainty that the relay does not record your traffic.

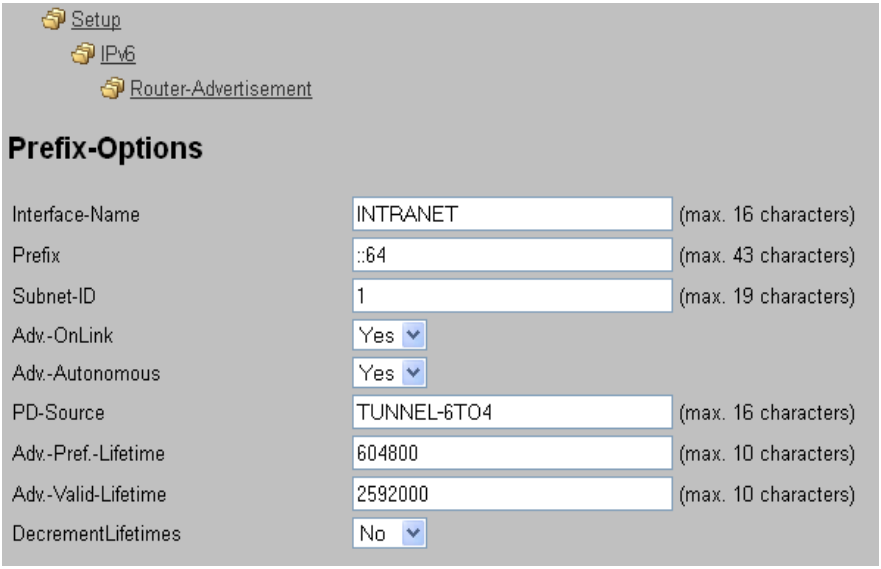
☐ In the field „IPv4-Rtg-tag“ accept the default value "0"

☐ Enable the „firewall“ for this tunnel.

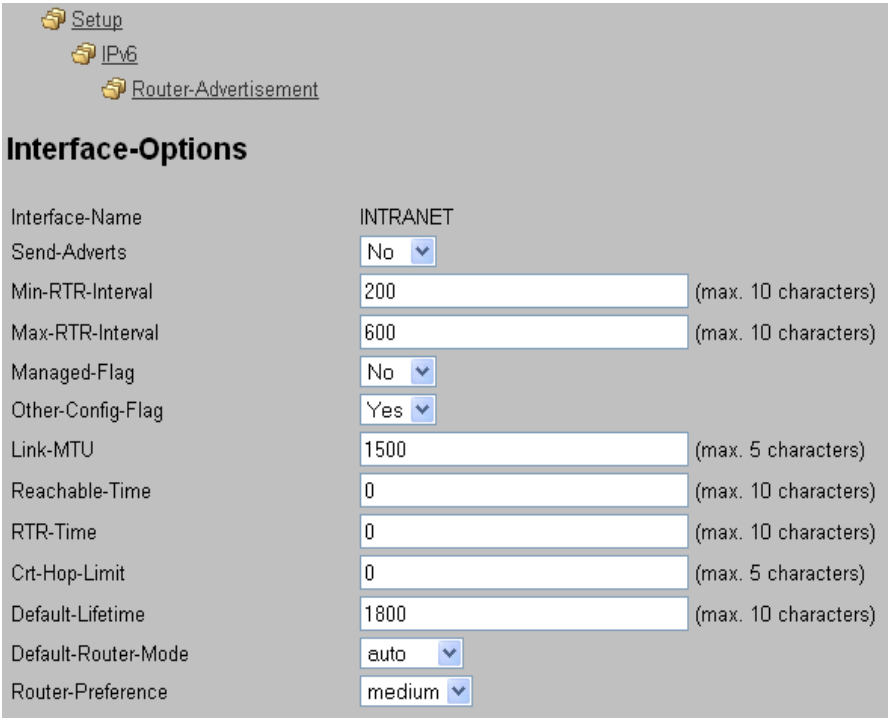
Hinweis: If you disable the global firewall, you should also disable the firewall for the tunnel.

☐ Save your entries with „Send“.

☐ Change to the directory `HiLCOS Menu Tree:Setup:IPv6:Router advertisement`, open the „Prefix options“ table and click „Add“.



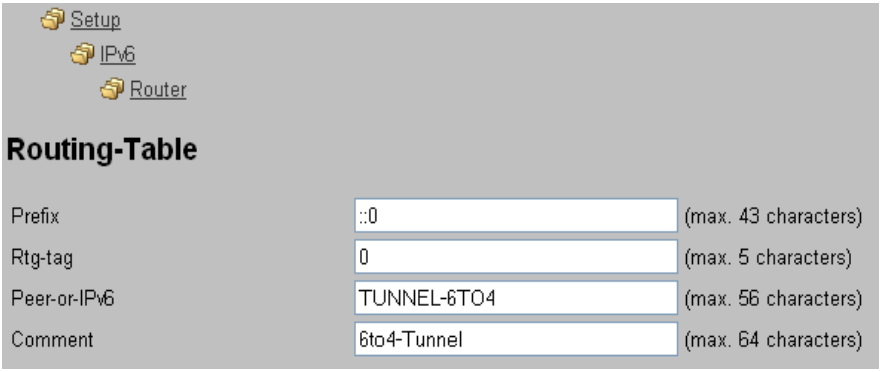
- ☐ Enter a name for the interface that uses the 6to4 tunnel, e.g. "INTRANET".
- ☐ Set the value for the „Prefix“ to "::/64" in order to accept the prefix issued by the provider automatically and in its entirety.
- ☐ Accept the default value of "1" for the „Subnet ID“.
- ☐ Set „PD source“ to the name of the remote peer that you previously defined in the example above, e.g. "TUNNEL-6TO4".
- ☐ Save your entries with „Send“.
- ☐ Change to the directory `HiLCOS Menu Tree:Setup:IPv6:Router advertisement`, open the „Interface options“ table and click „Add“.



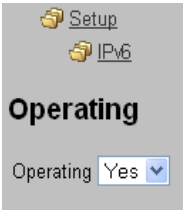
☐ Accept all other default values ??without change.

☐ Save your entries with „Send“.

☐ Change to the directory `HiLCOS Menu Tree:Setup:IPv6:Router`, open the „Routing table“ and click „Add“.



- ☐ Set the „Prefix“ to the value "::/0".
- ☐ In the field „Rtg-tag“ accept the default value "0".
- ☐ In the field „Peer or IPv6“, enter the name of the interface that will use the 6to4 tunnel, e.g. "TUNNEL-6TO4" in the example above.
- ☐ Enter a descriptive „Comment “for this entry.
- ☐ Save your entries with „Send“.
- ☐ Enable the IPv6 stack under `HiLCOS Menu Tree:Setup:IPv6` by setting the option „Operating“ to "yes" and save with „Send“.



13 Quality of Service

Quality of Service (QoS) refers to two different aspects of communication performance:

- Applying pre-defined transmission priorities to communications relating to different applications or sources, and
- defining a transfer type for a particular data source.

13.1 QoS Objectives

The main objective of QoS is to transfer specified data packets either as securely or as quickly as possible.

13.2 Which packets to prioritize?

The QoS concept arises from the condition of bandwidth scarcity: available bandwidth is not always sufficient to transmit all sent data packets reliably and on time. Load peaks can result from simultaneously downloading large ftp files, exchanging e-mails, and operating VoIP telephones over the data line. In order to balance these competing demands for bandwidth, certain data packets should be treated preferentially.

There are two ways to mark a data packet for preferential treatment by the OpenBAT device:

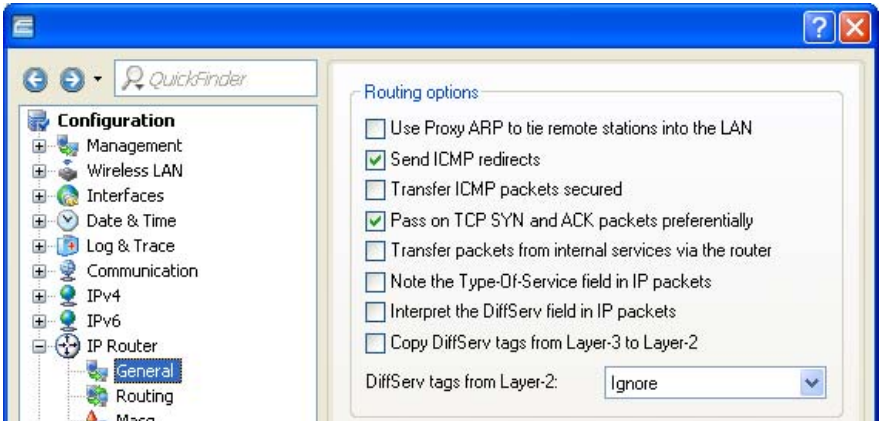
- The application, e.g., software operating in certain IP telephones, can mark the data packets appropriately. A tag is set within the header of the IP packets. The two different variants of this marking—ToS and DiffServ—assume the following states.
  - ToS “Low Delay“
  - ToS “High Reliability“
  - DiffServ “Expedited Forwarding“
  - DiffServ “Assured Forwarding“
- When the application itself cannot mark the data packets appropriately, the OpenBAT device can do so. It uses the existing functions of the firewall, which can classify data packets—for example, according to subnets or services (applications). Using these functions the OpenBAT device can mark data packets of an FTP connection or of a certain department (in a separate subnet) for prioritized treatment. For treatment of data packets classified by the firewall, the following two possibilities can be chosen:
  - Grant minimum bandwidth
  - Limited maximum bandwidth

13.3 Configuration of QoS

13.3.1 Evaluating ToS and DiffServ fields

ToS or DiffServ?

QoS is enabled if you have specified data packets for which the OpenBAT device issues priorities. This setting is made in LANconfig in the `Configuration : IP Router : General` dialog.



☐ Specify a QoS protocol, by making one of the following selections:

– Select "Note the Type-Of-Service Field in IP packets" to enable ToS checking. The OpenBAT device checks the bits for particularly fast or secured transmission.

– Select "Interpret the DiffServ field in IP packets" to enable DiffServ checking. The OpenBAT device checks the bits for Class Selector, Assured Forwarding, and Expedited Forwarding settings.

– To disable QoS, de-select both of the above settings (the default setting).

DiffServ in Firewall Rules

The code points from the DiffServ field can be evaluated by firewall rules for further control of QoS parameters such as minimum bandwidth or PMTU reduction. IP packets can be marked with DiffServ codepoints from suitable hardware (e.g. IP telephones) or applications (e.g. video telephony).

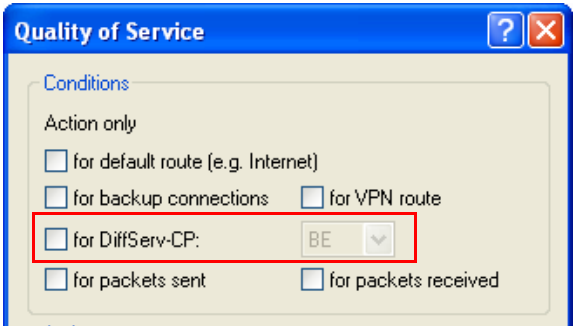
To create rules that give priority to specified DiffServ code points, follow these steps:

☐ Navigate to the following dialog:`Configuration : Firewall/QoS : IPv4 Rules` and click "Rules".

☐ In the ‘Firewall Rules’ list click ‘Add...’.

☐ In the ‘New Filter Rule’ dialog, select the ‘QoS’ tab.

☐ In the ‘QoS’ dialog, click ‘Add...’ then select ‘Add custom QoS’ to open the ‘Quality of Service’ dialog:



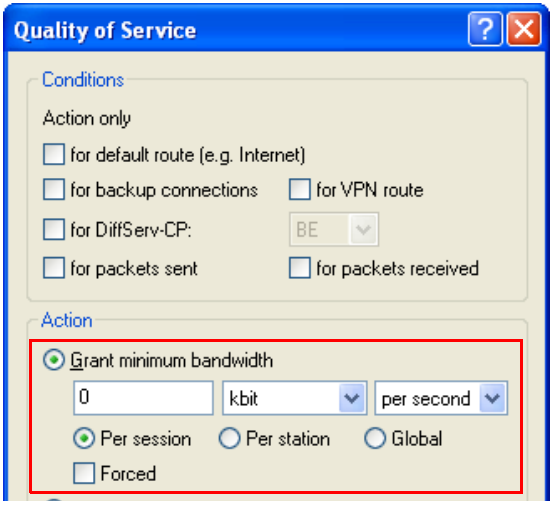
☐ Enable the setting "for DiffServ-CP" and choose from the dropdown list between:
- BE (Best Effort): Normal packet (corresponds CS0)
- CS (Class selector): 0 - 7 Is compatible to the TOS field of the IPv4 header and corresponds to the precedence of unset TOS bits
- AF (Assured forwarding): 0 - 4 / 0 - 3 The first digit represents the process priority and the second one represents the drop probability. The higher the priority and the lower the drop probability, the less frequently a packet will actually be dropped.
- EF (Expedited Forwarding): Self declaring.
- Value: An arbitrary tag—from 0 to 63—can be added.

Note: For additional information on how to configure firewall rules, refer to the chapter Firewall Configuration: LANconfig (see on page 697).

13.3.2 Granting Minimum Bandwidths

With the minimum bandwidth, you define how many packets will be transmitted with priority. The preference is active as long as the bandwidth limit is not exceeded. If the bandwidth is exceeded, the excess packets are transmitted, dropped or rejected as specified by other actions and rules. If no other applicable rule is configured, the corresponding packets are transmitted without preference.

You can create a grant of minimum bandwidth to selected transmissions in the ‘Quality of Service’ dialog. (Refer to the previous topic for the path to this dialog.)



To configure a firewall rule granting minimum bandwidth, configure the following parameters:

☐ Grant minimum bandwidth: Define the minimum bandwidth grant using the following elements:
- a numeric value: This field accepts SI prefixes (k, Ki, M, Mi, G, Gi) as well as the SI unit bit, which will divide the value by 8 when exiting the entry field.
- a unit of measure: kbit, kByte, packets, sessions, %bandwidth
- a measure of time: absolute, per hour, per minute, per second

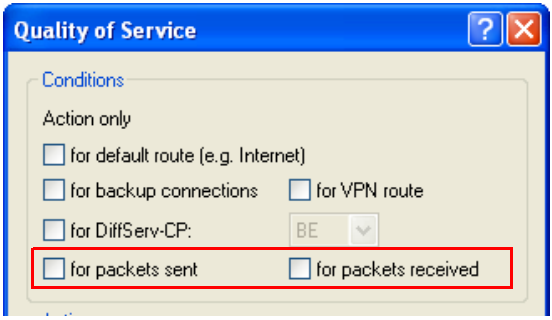
- ☐ The scope of the grant: Per session, Per station, Global
- ☐ Forced: This option exclusively reserves the specified bandwidth for each new session that matches this rule. The bandwidth is reserved for the entire duration of the session, even if the session temporarily requires less bandwidth. If the specified bandwidth is not available for a new rule matching session, the request to establish a connection is rejected.

Note: In addition to these settings, all other firewall rule parameters also apply to the grant of minimum bandwidth. Further information about configuring the firewall you find in 11 (see on page 697).

13.3.3 Configuring the send/receive direction

The OpenBAT configured by default to set the direction of the connection like the logical direction of the connection. You can change this default setting for the QoS firewall rule in the "Quality of Service" dialog.

- ☐ Navigate to the following dialog:`Configuration : Firewall/QoS : IPv4 Rules` and click "Rules".
- ☐ In the ‘Firewall Rules’ list click ‘Add...’.
- ☐ In the ‘New Filter Rule’ dialog, select the ‘QoS’ tab.
- ☐ In the ‘QoS’ dialog, click ‘Add...’ then select ‘Add custom QoS’ to open the ‘Quality of Service’ dialog:



☐ To configure the send/receive direction for packets with QoS tagging, do one of the following:

- Select "for packets sent" to apply the QoS firewall rule to packets physically sent from the LAN through the OpenBAT device.
- Select "for packets received" to apply the QoS firewall rule to packets physically received by the OpenBAT device and then forwarded to the LAN.

Note: For configuration with WEBconfig or Telnet, the interpretation of the data transfer direction is specified in a new firewall rule by parameters ‘R’ for receive, ‘T’ for transmit (send) and ‘W’ for reference to the WAN interface. For example, a limitation of the transmitted data to 16 KBit/s, based onto the physical WAN interface, can be achieved by the firewall rule `%Lcdstw16%d`.

13.3.4 Reducing Packet Length

You can increase the effectiveness of the QoS prioritization by reducing the length of the packets sent by the OpenBAT device. Extra-long packets can reduce the performance of QoS in prioritizing preferred packets.

Note: The packet length reducing firewall rule applies globally to all packets passing through the specified interface, regardless of protocol.

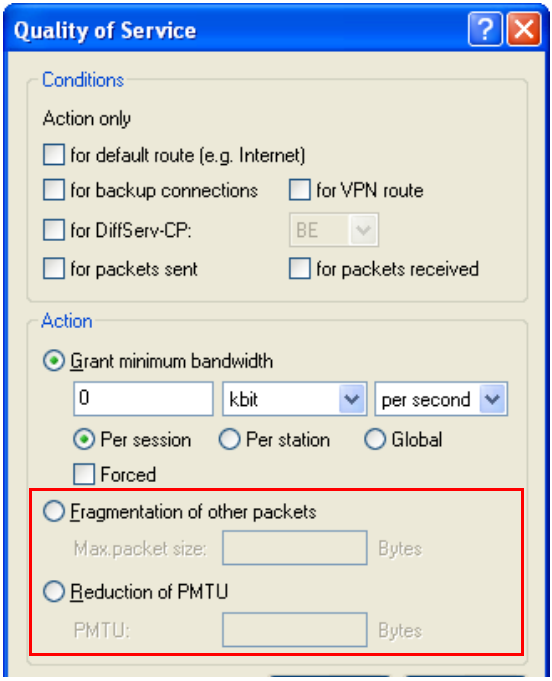
You can configure reduced packet length in the ‘Quality of Service’ dialog.

☐ Navigate to the following dialog:`Configuration : Firewall/QoS : IPv4 Rules` and click Rules.

☐ In the ‘Firewall Rules’ list click ‘Add...’.

☐ In the ‘New Filter Rule’ dialog, select the ‘QoS’ tab.

☐ In the ‘QoS’ dialog, click ‘Add...’ then select ‘Add custom QoS’ to open the ‘Quality of Service’ dialog:



To configure the send/receive direction for packets with QoS tagging, do one of the following:

- Select ‘Fragmentation of other packets’, then type in a ‘Maximum packet size’ (in Bytes). Packets larger than this size are subject to the rule, and will be handled according to the action defined for the rule.
- Select ‘Reduction of PMTU’ then type in a ‘PMTU’ (in Bytes) to establish the maximum transmission unit size for this path. Stations configured with the rule will adjust unit size to match this limit.

Note:

- For configuration with WEBconfig or Telnet, the reduction is entered in a new firewall rule by parameter “P” for PMTU reduction (Path MTU, MTU = Maximum Transmission Unit) and “F” for the fragment size.
- PMTU reduction and fragmentation always refer to the physical connection. Using the parameter “W” to represent the WAN sending direction is not required here and hence will be ignored if used.

The following example shows a setting for Voice over IP telephony:

Rule	Source	Destination	Action	Protocol
VOIP	IP addresses of IP telephones in the LAN, all ports	IP addresses of IP telephones in the LAN, all ports	%Qcds32 %Prt256	UDP

This rule defines the minimum bandwidth for sending and receiving 32 Kbps, forces and reduces the PMTU while sending and receiving to packets of 256 byte size. For the TCP connection, the maximum segment size of the local workstation is set at 216, so that the server will send packets of maximum 256 byte (reduction of the PMTU in sending and receiving direction).

13.4 QoS for WLANs: IEEE802.11e (WMM/WME)

Based on the 802.11e standard, QoS can be applied to WLAN transfers. The 802.11e standard supports, among other things, the prioritization of certain data-packet types. This extension of the 802.11 standard is an important basis for the use of voice applications in WLANs (Voice over WLAN, VoWLAN).

The WiFi alliance certifies products that support QoS according to 802.11e, and refer to WMM (WiFi Multimedia, formerly known as WME or Wireless Multimedia Extension). WMM defines four categories (voice, video, best effort and background) that constitute separate queues to be used for prioritization.

The 802.11e standard sets priorities by referring to the WLAN tags or, in the absence of these, by the DiffServ fields of IP packets. Delay times (jitter) are kept below 2 milliseconds, a magnitude which is inaudible to the human ear. 802.11e controls access to the transfer medium with EDCF, the Enhanced Distributed Coordination Function.

Note: Both of the following are preconditions to setting priorities:
- both the WLAN client and the access point support 802.11e or WMM
- the applications need to be able to mark the data packets with the corresponding priorities

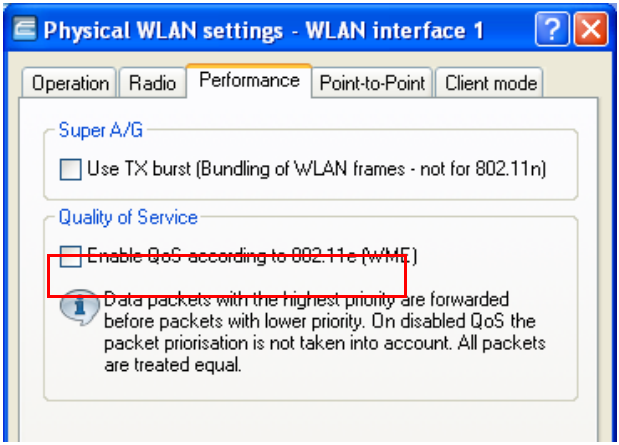
You can configure the OpenBAT device to separately activate 802.11e for each of its physical WLAN networks. Do the following:

☐ Open `Configuration : Wireless LAN : General`

☐ Click ‘Physical WLAN settings’ and select an interface

☐ In the ‘Physical WLAN settings’ dialog, select the ‘Performance’ tab.

☐ Select ‘Enable QoS according to 802.11e (WME)’


Physical WLAN settings - WLAN interface 1
Operation
Radio
Performance
Point-to-Point
Client mode
Super A/G
Use TX burst (Bundling of WLAN frames - not for 802.11n)
Quality of Service
Enable QoS according to 802.11e (WME)
Data packets with the highest priority are forwarded before packets with lower priority. On disabled QoS the packet priorisation is not taken into account. All packets are treated equal.

14 Additional Services

OpenBAT devices offer the additional services described in this chapter.

14.1 IP Address Administration via DHCP

14.1.1 Introduction

DHCP Server

All devices in a TCP/IP LAN require a unique IP address. They also may need the addresses of Domain Name System (DNS) and NetBIOS Name (NBNS) servers, and a standard gateway that can route data packets to addresses not located on the local network.

In a small network it is possible to manually enter these addresses on all the computers in the network. However, in a large network with many workstations this quickly becomes an unmanageable task. In the case of large networks, administrators typically use a DHCP server to dynamically assign the required addresses to individual workstations.

These OpenBATdevices come equipped with an integrated DHCP server that can take on the task of assigning IP addresses in the LAN. This process involves communicating the following parameters to the workstations:
- IP address
- Network mask
- Broadcast address
- Standard gateway
- DNS server
- NBNS server
- Lease (validity period) of the assigned parameters

The DHCP server either takes the IP addresses from a freely defined address pool or determines the addresses independently based on its own IP address. An unconfigured device in DHCP auto-mode can autonomously specify IP addresses for itself and for other network devices.

In the simplest scenario, you just need to connect a new out-of-the-box OpenBAT device to a network that has no other DHCP server and switch it on. The integrated DHCP server in the OpenBAT device manages all subsequent IP address assignment in the LAN, in cooperation with LANconfig wizards.

Note: DHCP settings can differ for each network. It is possible to define several IP networks in the OpenBAT devices in conjunction with advanced routing and forwarding (ARF). Thus, with the exception of a few general settings, DHCP settings apply to just a particular IP network.

DHCP Relay

If another DHCP server is located in the LAN, the OpenBAT device—if it is operating in client mode—can obtain its required address information from the other DHCP server.

The OpenBAT can operate as a DHCP relay agent and as a DHCP relay server:

- As a DHCP relay agent the OpenBAT device forwards DHCP requests to another DHCP server.
- As a DHCP relay server the OpenBAT device processes DHCP requests forwarded from DHCP relay agents.

BOOTP

The bootstrap protocol (BOOTP) can be used to send a specified IP address and other parameters to a workstation when it boots up. Workstations without hard drives can use BOOTP to load a boot image—i.e. a complete operating configuration—from a boot server.

14.1.2 Configuring DHCP parameters in LANconfig

Activating a DHCP Server for a Selected Logical Interface

The DHCP server can be activated or deactivated separately for each logical interface (e.g. LAN-1, WLAN-1, P2P-1-1 etc.). To do this:

☐ Navigate to the following dialog:`Configuration : IPv4 : DHCPv4.`

☐ Click "Port table" and select a logical interface from the list to open the following dialog, where you can enable and disable the DHCP server for this interface:

Configuring DHCP Networks

DHCP settings can be specified separately for any IP network defined in the OpenBAT device. As part of configuring DHCP networks, you need to define a range of addresses (an address pool) that can be assigned to DHCP clients.

When a client is activated in the network and requests an IP address via DHCP, the OpenBAT device with an activated DHCP server offers to issue an address. This address is selected from the pool of valid IP addresses. A computer that has received a specific IP address in the past requests the same address again and—if the DHCP server has not reassigned this address to another computer—the server attempts to issue the client its previous address.

The DHCP server also checks the LAN to confirm that the selected address is available. If the address is confirmed as unique, it is assigned to the requesting computer.

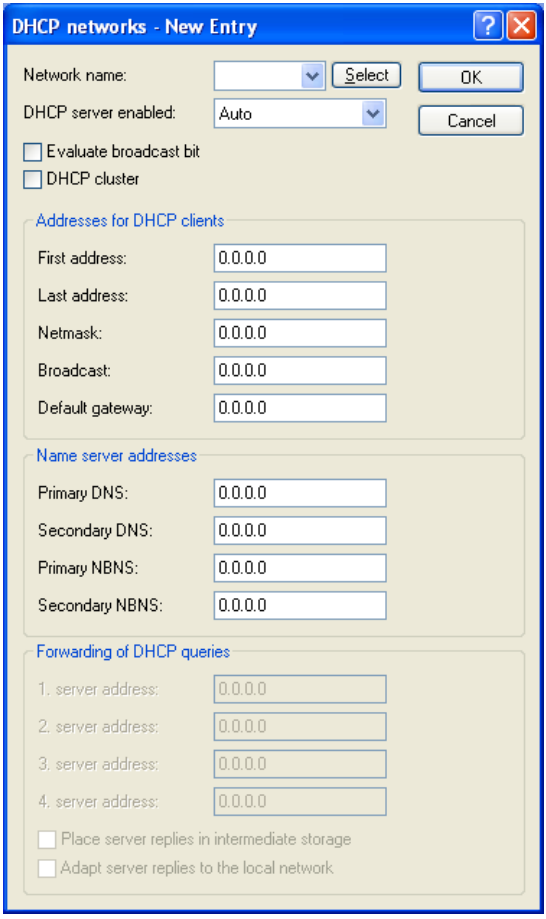
Note:

- The device factory settings include the IP networks "Intranet" and "DMZ," although there are no settings for IP addresses and netmasks. In the absence of a pre-existing address for networked devices, the OpenBAT device uses the IP address '172.23.56.254' for itself, and the address pool '172.23.56.x' for assigning IP addresses to the network.
- With the configuration of IP and DHCP networks, multiple networks with different DHCP settings can be active on the same logical interface. In this case, the DHCP settings for the first suitable network are applied. A prioritization of networks may be necessary.

To configure a DHCP network, follow these steps:

☐ Navigate to the following dialog:`Configuration : IPv4 : DHCPv4` and click "IP networks".

☐ In the ‘DHCP networks’ table, either select an existing network and click ‘Edit...’ or click ‘Add...’ to create a new DHCP network:



Configure the DHCP network by entering values for the following settings:

- Network name:
  Select the IP network for these DHCP settings.

  Note: Navigate to the following dialog:`Configuration : IPv4 : General` to add new IP networks if necessary.

- DHCP server enabled:
  Select a mode of operation:
  - No: The DHCP server is disabled.
  - Yes: The DHCP server is enabled. Use this setting if you are certain that no other DHCP server is active in the LAN. When this value is entered the server configuration (validity of the address pool) is checked:
    – If the configuration is correct then the device starts operating as a DHCP server in the network.
    – An incorrect DHCP configuration (e.g. invalid pool limits) will disable the DHCP server.
  - Auto (default): The device regularly searches the local network for other DHCP servers. The LAN-Rx/Tx LED flashes briefly when this search is in progress.
    – If another DHCP server is discovered, the device switches its own DHCP server off. If the OpenBAT device is not configured with an IP address, then it switches into DHCP client mode and queries the LAN DHCP server for an IP address. Unconfigured devices introduced to the network cannot assign addresses unintentionally.OpenBAT
    – If no other DHCP servers are discovered, the device switches its own DHCP server on. If another DHCP server is activated later, then the DHCP server in the OpenBAT device will be disabled.
  - Client Mode: The DHCP server is disabled, the device behaves as a DHCP client and obtains its address from another DHCP server in the LAN. Use this setting if you are certain that another DHCP server is in the LAN and actively assigning IP addresses.
  - Forward queries: The DHCP server is enabled and receives requests from DHCP clients in the LAN. The device does not respond to requests itself, but forwards them to a central DHCP server in a different network segment.
- Evaluate broadcast bit:
  Select this to have the DHCP server evaluate the broadcast bit sent by the client. If the bit is not evaluated, then all DHCP responses are sent as broadcasts.

- DHCP cluster:
  Select this to have the DHCP server track running DHCP negotiations, adding hosts to its own table, including those that are registered to other DHCP servers. In this way, the DNS server can resolve the names of hosts registered to any member of the cluster.
- First / Last address:
  Use these parameters to define the IP address pool, as follows:
  - Create a range of IP address values to create an IP address pool; or
  - Enter a value of '0.0.0.0' in each field, to have the DHCP server determine the relevant first and last addresses itself using the settings for the IP network (network address and netmask).

  Note: Recall that the device is in a special operating mode if no IP network has yet been defined. In that case, it uses the IP address '172.23.56.254' and the address pool '172.23.56.x' for assigning IP addresses to the network.
- Netmask:
  The netmask is assigned in a similar way to assigning addresses. If a netmask has been entered here, it will be used when assignment is made. Otherwise the IP network's netmask will be used.
- Broadcast:
  Do one of the following:
  - Leave this field blank: the broadcast address is determined using the device's own address and netmask, if possible.
  - Enter an IP address: In special cases (e.g. when using subnets for a selection of workstations) it may be necessary to use a different broadcast address. In this case enter that broadcast address here.

  Note: Experienced personnel exclusively should change the setting for the broadcast address.
- Default gateway:
  Normally, the address of this device is transferred to the stations as the standard gateway. To select a different standard gateway, enter its IP address here.

- Primary / Secondary DNS:
  Enter the address of a name server to which DNS queries should be forwarded. These fields may be left blank if you have an Internet provider or other remote station that automatically assigns a name server when logging in.
- primary / Secondary NBNS:
  Enter the address of a name server to which NBNS queries should be forwarded. These fields may be left blank if you have an Internet provider or other remote station that automatically assigns a name server when logging in.
- 1-4 server address:
  If the forwarding of DHCP queries is enabled, enter the IP addresses of the upstream DHCP servers here. These servers do not have to be located in the local network. Requests sent as broadcasts are forwarded to configured DHCP servers. You can enter directly the IP address of the particular server or the broadcast address of the network in which the server is located.
- Place server replies in intermediate storage:
  If this option is enabled, the device buffers the responses from the upstream DHCP server in order to respond directly to subsequent queries. Unnecessary connections can thus be avoided if the upstream server is located in a remote network.
- Adapt server replies to the local network:
  If this option is enabled, the device modifies the replies from the upstream DHCP server to adapt them to the local network. This involves replacing the Standard Gateway, DNS Server and NBNS Server values.

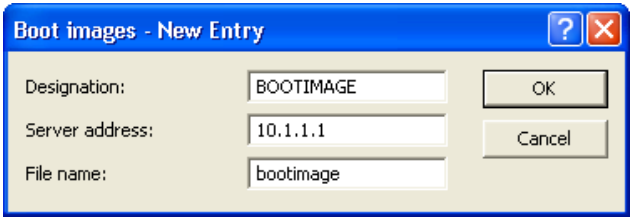
Assigning fixed IP addresses and boot images to clients

You can use LANconfig to create boot images for DHCP clients, then assign both that boot image and a fixed IP address to selected DCP clients.

To create a boot image:

☐ Navigate to the following dialog:`Configuration : IPv4 : BOOTP` and click "Boot images".

☐ In the ‘Boot images’ window, click ‘Add...’ to create a new entry:



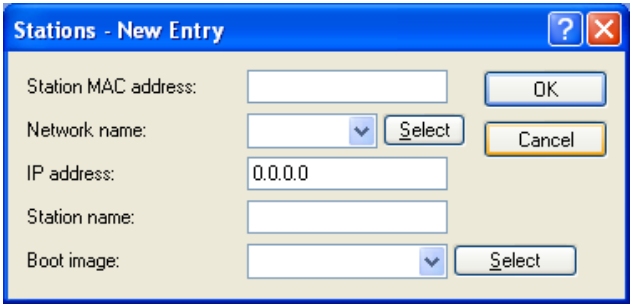
Enter settings for these parameters:

- Designation:
  Input a name for this boot image. This name will be used when assigning a boot image to a specific station in the station list.
- Server address:
  Enter the IP address of the server providing the boot image.
- File name:
  Specify the name of the file on the server that contains the boot image.

To assign a fixed IP address and (optionally) a boot image to a client:

☐ Navigate to the following dialog:`Configuration : IPv4 : BOOTP` and click "Stations".

☐ In the ‘Stations’ window, click ‘Add...’ to create a new entry:



Enter settings for these parameters:

- Station MAC address:
  Specify the MAC address (node ID) of the station's network adapter.
- Network name:
  Select the network name of the ARF network, for which these settings should apply. If this field is left empty, the device allocates the configured address from the ARF network from which the DHCP request took place. If the request derives from an ARF network for which no particular address has been configured, the device assigns an address dynamically from the address pool.

  Note: If the assigned IP address is not part of the address range of the configured ARF network, the assignment will be discarded and instead an IP address will be chosen from the address range of the ARF network from which the request took place.
- IP address:
  Enter the IP address to be assigned.
- Station name:
  Enter a name to identify the station. If a station does not transfer its name, the device will use the name entered here.
- Boot image (optional):
  Selected the image file that contains the station's operating system. The client needs to support the BOOTP protocol.

14.1.3 Configuring DHCP parameters via WEBconfig or Telnet

DHCP configuration and status parameters can also be accessed using either Telnet or WEBconfig.

DHCP configuration parameters can be accessed at:

```
HiLCOS Menu Tree : Setup : DHCP
```

Configurable DHCP settings in WEBconfig include:

- General DHCP settings
- Alias list
- Hosts table
- Network list
- Port table
- Additional options

DHCP status parameters are found in the be accessed at:

```
HiLCOS Menu Tree : Status : TCP/IP : DHCP : DHCP Table
HiLCOS menu tree : Setup : DHCP : DHCP table
```

General DHCP Statistics

This table contains information on IGMP packets. Field values include:

- User class identifier: The DHCP client in the OpenBAT device can insert additional information in the DHCP request sent, which simplifies recognition of requests within the network. The vendor class identifier (DHCP option 60) shows the device type, and is included in the transmission. The user class ID (DHCP option 77) specifies a user-defined string, and is transmitted when the user has configured a value.
- Default lease time minutes:
  When a client requests an address without asking for a specific lease, the address will be assigned this value as its lease.
- Max lease time minutes:
  When a client requests an IP address from a DHCP server, it can also ask for a lease for the address. This value governs the maximum length of lease that the client may request.

Alias List

The alias list defines the names for the boot images that are used to reference the images in the hosts table:

- Image alias:
  Enter any name you wish for this boot image. This name is used when you assign a boot image to a particular client in the station list.
- Image server:
  Enter the IP address of the server that provides the boot image.
- Image file:
  Enter the name of the file on the server containing the boot image.

Hosts Table

The bootstrap protocol (BOOTP) can be used to communicate a certain IP address and other parameters to a workstation when it boots up. To enable the initial communication, the workstation's MAC address is required.

- MAC address:
  Enter the MAC address of the workstation to which an IP address is to be assigned.
- Network name:
  Enter the name of a configured IP network here. A requesting client needs to be located in this IP network to be assigned the relevant IP address defined for the MAC address.

  Note: If the requesting client is located in an IP network for which there is no corresponding entry in the hosts table, the client will be assigned an IP address from the address pool of the appropriate IP network.
- IP address:
  Enter the client IP address that is to be assigned to the client.
- Hostname:
  Enter the name that is to be used to identify the client. If the client does not communicate its name, the device will use this name.
- Image alias:
  If the client uses the BOOTP protocol, you can select a boot image that the client should use from which to obtain its operating system.

Note: Enter the name of the server providing the boot image and the name of the file on the server in the boot image table.

Network List

DHCP settings for the IP networks are defined in this table.

- Network name:
  The name of the network to which the DHCP server settings apply.
- Operating:
  - No: The DHCP server is disabled.
  - Yes: The DHCP server is enabled. Use this setting if you are certain that no other DHCP server is active in the LAN. When this value is entered the server configuration (validity of the address pool) is checked:
    – If the configuration is correct then the device starts operating as a DHCP server in the network.
    – An incorrect DHCP configuration (e.g. invalid pool limits) will disable the DHCP server.
  - Auto (default): The device regularly searches the local network for other DHCP servers. The LAN-Rx/Tx LED flashes briefly when this search is in progress.
    – If another DHCP server is discovered, the device switches its own DHCP server off. If the OpenBAT device is not configured with an IP address, then it switches into DHCP client mode and queries the LAN DHCP server for an IP address. Unconfigured devices introduced to the network cannot assign addresses unintentionally.OpenBAT
    – If no other DHCP servers are discovered, the device switches its own DHCP server on. If another DHCP server is activated later, then the DHCP server in the OpenBAT device will be disabled.

- Client Mode: The DHCP server is disabled, the device behaves as a DHCP client and obtains its address from another DHCP server in the LAN. Use this setting if you are certain that another DHCP server is in the LAN and actively assigning IP addresses.
- Relay: The DHCP server is enabled and receives requests from DHCP clients in the LAN. The device does not respond to requests itself, but forwards them to a central DHCP server in a different network segment.

- Evaluate broadcast bit:
  Select this to have the DHCP server evaluate the broadcast bit sent by the client. If the bit is not evaluated, then all DHCP responses are sent as broadcasts.
- Start address pool:
  The first IP address in the pool available to the clients. If no address is entered here the DHCP takes the first available IP address from the network (as determined by network address and netmask).
- End address pool:
  The last IP address in the pool available to the clients. If no address is entered here the DHCP takes the first available IP address from the network (as determined by network address and netmask).
- Netmask:
  Corresponding netmask for the address pool available to the clients. If no address is entered here the DHCP server uses the netmask from the corresponding network.
- Broadcast address:
  As a rule, broadcast packets in a local network have an address which results from the valid IP addresses and the netmask. In special cases (e.g. when using subnets for a selection of workstations) it may be necessary to use a different broadcast address. In this case the broadcast address is entered into the DHCP module.

  Note: Experienced personnel exclusively should change the setting for the broadcast address.

- Gateway address: By default, the
  OpenBAT device issues its own IP address as the gateway address to computers making requests. If necessary, the IP address of another gateway can be transmitted if a corresponding address is entered.

- DNS default:
  IP address of the DNS name server for the forwarding of DNS requests.
- DNS backup:
  IP address of the backup DNS name server for the forwarding of DNS requests, in the event that the first named server ceases to operate.
- NBNS default:
  IP address of the NBNS name server for the forwarding of DNS requests.
- NBNS backup:
  IP address of the backup NBNS name server for the forwarding of DNS requests, in the event that the first named server ceases to operate.
- Master server / 2nd / 3rd / 4th master server:
  This is where the IP address for the superordinate DHCP servers can be entered when the mode 'Relay requests' is selected.
- Place server replies in intermediate storage:
  This option allows the responses from the higher-level DHCP server to be stored in the OpenBAT device. Subsequent requests can then be answered by the OpenBAT device itself. This option is useful if the higher-level DHCP server can be reached exclusively via a connection that incurs costs.
- Adaptation of server response to the local network:
  This option allows the responses from the higher-level DHCP server to be adapted to the local network. When activated, the OpenBAT device adapts the responses from the higher-level DHCP server by replacing the following entries with its own address (or locally configured addresses):
  – Gateway
  – Network mask
  – Broadcast address
  – DNS server
  – NBNS server
  – Server ID

This option is worthwhile if the superordinate DHCP server does not permit the separate configuration for DHCP clients in another network.

- Cluster:
  This option lets you ‘cluster’ multiple DHCP servers, causing them to work together to provide uninterrupted DHCP services in the event a single server ceases to function.

Port Table

The port table is where the DHCP server is enabled for the appropriate logical interface of the device.

- Port:
  Select the logical interface for which the DHCP server should be enabled or disabled.
- Enable DHCP:
  Enables or disables the DHCP server for the selected logical interface.

Additional Options

DHCP options can be used to send additional configuration parameters to the clients. The vendor class ID (DHCP option 60) shows, for example, the type of device. This table allows additional options for DHCP operations to be defined.

- Option number:
  Number of the option that should be sent to the DHCP client. The option number describes the transmitted information. For example ‘17’ (root path) is the path to a boot image that a PC without its own hard disk uses to obtain its operating system via BOOTP. You can find a complete list of DHCP options in RFC 2132 – ’DHCP Options and BOOTP Vendor Extensions’ of the Internet Engineering Task Force (IETF).
- Network name:
  Name of the IP network where this DHCP option is to be used.

- Option type:
  Description of the DHCP option type.
- Option value:
  This field defines the contents of the DHCP option. For the option ‘17’ for example, the path is entered for a boot image that a PC without its own hard disk uses to obtain its operating system via BOOTP.

DHCP Table

The DHCP table provides an overview of the IP addresses used in the IP networks. The DHCP table is purely a status table where no parameters can be configured.

- IP address:
  IP address the DHCP server has assigned to the station.
- MAC address:
  The client's MAC address.
- Timeout:
  Period of validity (lease) for the address assignment in minutes.
- Hostname:
  Name of the client, if it was possible to determine this.
- Type:
  The 'Type' field indicates how the address was assigned. This field may contain the following values:
  - New: The client made the request for the first time. The DHCP checks that the address to be assigned to the client is unique.
  - Unknown: When the server checked if the address was unique, it was found that the address had already been assigned to another client. As a result, the server can obtain no additional information.
  - Stat: A client has informed the DHCP server that it has a fixed IP address. Because an IP address is defined as unique, this IP address is reserved exclusively for this client.
  - Dyn.: The DHCP server has assigned an address to the client.
  - Cache: The DHCP server has assigned an address from the cache to the client.

- LAN lfc:
  Logical interface connecting the client to the device.
- Ethernet port:
  Physical interface over which the DHCP server assigned the IP address to the station.
- VLAN ID:
  The VLAN ID used by the client.
- Network name:
  Name of the IP network where the client is located.
- Assignment:
  Point in time when the DHCP server assigned the IP address to the station

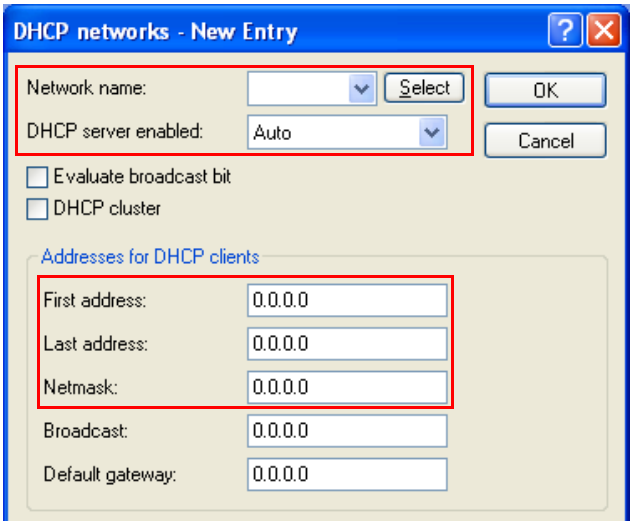
14.1.4 DHCP Relay Server

In addition to forwarding DHCP requests, a OpenBAT device is not limited to forwarding DHCP requests to higher-level DHCP servers; a OpenBAT device can also function as a central DHCP server (DHCP relay server). For a OpenBAT device to be configured as a DHCP relay server to other networks, enter the relay agent IP address (the gateway IP address—GI address) as the network name in the table of IP networks.

If the same network is being used by several relay agents (e.g. multiple access points are forwarding requests to a central DHCP server) then the GI address can also be abbreviated with an asterisk (*). If, for example, clients in the remote network "10.1.1.0/255.255.255.0" are to be assigned addresses and several relay agents are available in this network, all of which use the OpenBAT device as higher-level DHCP server, then the assignment of IP addresses and standard gateway to the clients can take place as follows:

☐ Navigate to the following dialog:`Configuration : IPv4 : DHCPv4` and click "IP networks".

☐ In the ‘DHCP networks’ dialog, either select an existing network and click ‘Edit...’ or click ‘Add...’ to create a new DHCP network.



In this example, enter values for at least the following fields:

- Network name: ‘10.1.1.*’
- DHCP server enabled: ‘Yes’
- First address ‘10.1.1.100’
- Last address: ‘10.1.1.105’
- Netmask: ‘255.255.255.0’

Note: To operate a DHCP relay server, define both the IP address range and the netmask.

- DNS Resolution of Names Learned via DHCP

  The DNS server considers the interface tags when resolving names learned via DHCP. The names to be resolved are exclusively those that were learned from a network with the same interface tag as the requesting computer. If the request arrives from an untagged network, then all names are resolved, including those that were learned via tagged networks. Similarly, all names that were learned from untagged networks are visible for tagged networks.

  Names learned from relay agents are handled as though they were learned from an untagged network. These names are visible to all networks.

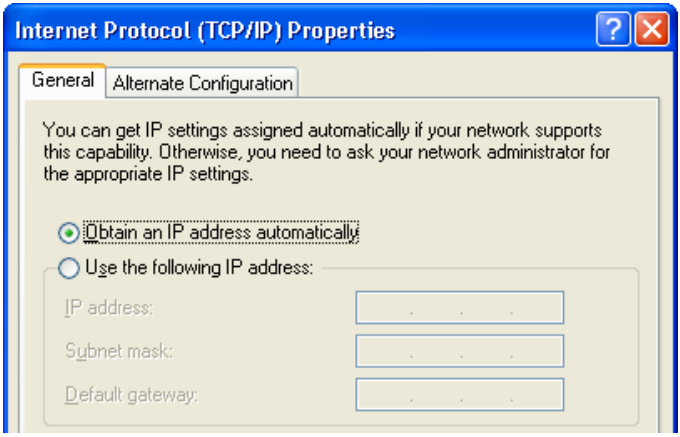
14.1.5 Configuring Clients

It is standard in a Windows network environment to configure settings so that parameters, which are necessary for device operation, can be requested via DHCP. To check your Windows settings, in your Windows desktop, select:

☐ Navigate to the Windows Control Panel and open the `Network Connections` dialog.

☐ Right click on a ‘Local Area Connection’ and select ‘Properties’ from the pop-up menu.

☐ Select ‘Internet protocol (TCP/IP)’ then click ‘Properties’ to open the ‘TCP/IP Properties’ dialog.


Internet Protocol (TCP/IP) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:

In the ‘General’ tab of this dialog, you can see if IP address settings are specially configured for this client, or if they are automatically obtained from a DHCP server.

If a client is to use different IP addressing parameters from the ones assigned (e.g. for a standard gateway), these need to be configured at the workstation itself. In that case, the client ignores the parameters assigned by the DHCP server.

14.1.6 Checking IP Addresses in the LAN

You can view a summary of the LAN IP addresses in the DHCP table at:

```
HiLCOS menu tree : Status : TCP/IP : DHCP : DHCP table
HiLCOS menu tree :Setup : DHCP : DHCP table
```

The DHCP table shows the assigned and used IP address, the MAC address, the lease, the client's name (if available) as well as the type of address assignment:

DHCP-Table

IP-Address	MAC-Address	Timeout	Hostname	Type	LAN-Ifc	Ethernet-Port	VLAN-ID	Network-name	Assignment
192.168.2.3	0001e37	441		dyn.	LAN-1	unbekannt	0	INTRANET	15.07.2013 12:35:52
192.168.2.28	848f69d1	393		dyn.	LAN-1	unbekannt	0	INTRANET	15.07.2013 13:29:48
192.168.2.29	0021709	94		dyn.	LAN-1	unbekannt	0	INTRANET	15.07.2013 09:45:41
192.168.2.56	bc47602	354		dyn.	LAN-1	unbekannt	0	INTRANET	15.07.2013 11:08:53
192.168.2.63	001f1fba	112		dyn.	LAN-1	unbekannt	0	INTRANET	15.07.2013 07:06:49
192.168.2.89	000085e	441		dyn.	LAN-1	unbekannt	0	INTRANET	15.07.2013 12:35:43
192.168.2.90	001d09d	422		dyn.	LAN-1	unbekannt	0	INTRANET	15.07.2013 13:30:27
192.168.2.98	74e2f50	4861		dyn.	LAN-1	unbekannt	0	INTRANET	14.07.2013 18:36:24
192.168.2.108	002170e	478		dyn.	LAN-1	unbekannt	0	INTRANET	15.07.2013 13:12:56
192.168.2.118	000c297	284		dyn.	LAN-1	unbekannt	0	INTRANET	15.07.2013 09:58:43

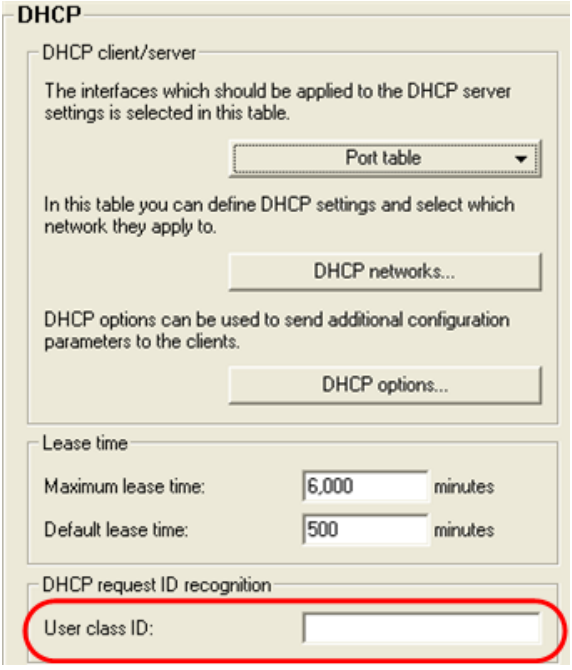
14.2 Vendor class and User class identifiers

The DHCP client in a OpenBAT device can insert additional information in the DHCP request sent, which simplifies request recognition within the network.

- The vendor class identifier (DHCP option 60) shows the device type. The vendor class ID is included in the transmission.
- The user class identifier (DHCP option 77) displays a user-defined string of up to 63 characters. The user class ID is transmitted when the user has configured a value.

To configure the user class ID:

☐ Navigate to the following dialog:`Configuration : IPv4 : DHCPv4` and enter a value into the field "User class ID".


DHCP
DHCP client/server
The interfaces which should be applied to the DHCP server settings is selected in this table.
Port table
In this table you can define DHCP settings and select which network they apply to.
DHCP networks...
DHCP options can be used to send additional configuration parameters to the clients.
DHCP options...
Lease time
Maximum lease time:
6,000
minutes
Default lease time:
500
minutes
DHCP request ID recognition
User class ID:

14.3 DNS

The domain name service (DNS) in TCP/IP networks is responsible for associating computer names to network (domain) and IP addresses. This service is required for Internet communications. It is also useful to be able to clearly associate IP addresses to computer names within a local network or in a LAN interconnection.

14.3.1 DNS Functions

The names used in DNS server requests consist of several parts:

- One part is the actual name of the host or service to be addressed.
- Another part specifies the domain.

Specifying the domain is optional within a local network. These names could thus be 'www.domain.com' or 'ftp.domain.com', for example.

If no DNS server exists in the local network, all locally unknown names are searched for using the default route. By using a DNS server, it is possible to go immediately to the correct remote station for all of the names with known IP addresses. In theory, the DNS server can be a separate computer in the network. However, locating the DNS server directly in the OpenBAT device is a better design, for the following reasons:

- The OpenBAT device can automatically distribute IP addresses to the computers in the LAN when operating as a DHCP server. It already knows the names and IP addresses of all of the computers in its own network that were assigned IP addresses via DHCP. Because of the dynamic address assignments by the DHCP server, an external DNS server might have difficulties in keeping the associations current between the names and IP addresses.
- When routing Microsoft Networks via NetBIOS, the OpenBAT device also knows the computer names and IP addresses in the other connected NetBIOS networks. In addition, computers with fixed IP addresses can also enter themselves in the NetBIOS table and thus be known by both their names and addresses.
- The DNS server in the OpenBAT device can also be used as an extremely convenient filter mechanism. Requests for domains can be prohibited throughout the LAN, for subnetworks, or even for individual computers —simply by specifying the domain name.

How the DNS Server Responds to Requests

When processing requests for specific names, the DNS server takes advantage of all of the information available to it:

- First, the DNS server determines whether access to the name is prohibited by the filter list. If that is the case, the DNS servers returns an exception response to the requesting computer stating that access to the address is denied.
- Next, the DNS server searches in its own static DNS table for suitable entries.
- If the address cannot be found in the DNS table, the DNS server searches the dynamic DHCP table. The use of DHCP information can be disabled.

- If no information for the name can be located in the previous tables, the DNS server searches the lists of the NetBIOS module. The use of the NetBIOS information can also be disabled if necessary.
- Finally, the DNS server checks whether the request is to be forwarded to another DNS server via a WAN interface (special DNS forwarding via the DNS destination table).

If the requested name cannot be found in any of the information sources available to it, the DNS server sends the request to another server—that of the Internet provider, for example—using the general DNS forwarding mechanism, or returns an exception response to the requesting computer.

14.3.2 DNS Forwarding

If it cannot serve the request from its own DNS tables, the DNS server forwards the request to other DNS servers. This process is called DNS forwarding. Note that there is a distinction between:

- Special forwarding: Requests for certain name areas are forwarded to certain DNS servers.
- General DNS forwarding: All other names not specified in detail are forwarded to the ‘higher-level’ DNS server.

Special DNS Forwarding

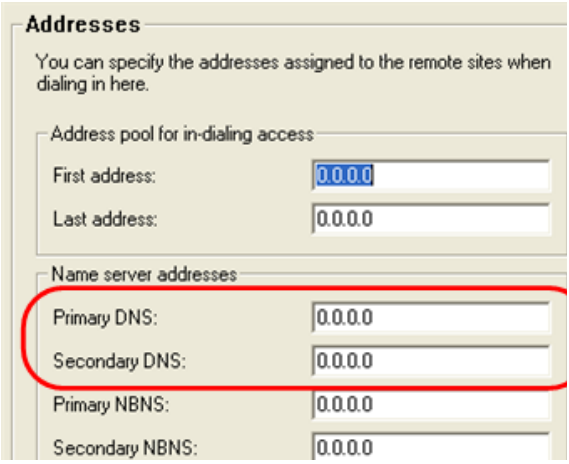
With special DNS forwarding, you can define name areas that can determine which specified DNS server is addressed. A typical application for special DNS involves the case of a home workstation. The user wants to be able to connect to the company intranet and directly to the Internet at the same time. The requests sent into the intranet need to be routed to the company DNS server, and other requests need to be routed to the DNS server of the provider.

General DNS Forwarding

DNS requests that cannot be resolved in another way are forwarded to a DNS server. The identity of this DNS server is determined according to the following rules:

- Initially, the router checks whether a DNS server has been identified in its own configuration settings. If so, it obtains the desired information from this server. Up to two higher-level DNS servers ('Primary DNS' and 'Secondary DNS') can be set in LANconfig at:

  ☐ `Configuration : IPv4 :Addresses.`



- If no DNS server has been identified in the device configuration, the router attempts to reach a DNS server over a PPP connection (e.g. from the Internet provider) to obtain the IP address assigned to the name. This can succeed if the address of a DNS server is sent to the router during PPP negotiation.
- If no such PPP connection exists, the default route is established and the DNS server searched for.

Entering the Intranet address of your router as the DNS server for the workstation computers is sufficient to enable you to obtain the name assignment. This procedure also automatically updates the address of the DNS server. Your local network receives the most current information even if, for example, the provider sending the address changes the name of his DNS server or you change to another provider.

14.3.3 Configuring the DNS Server

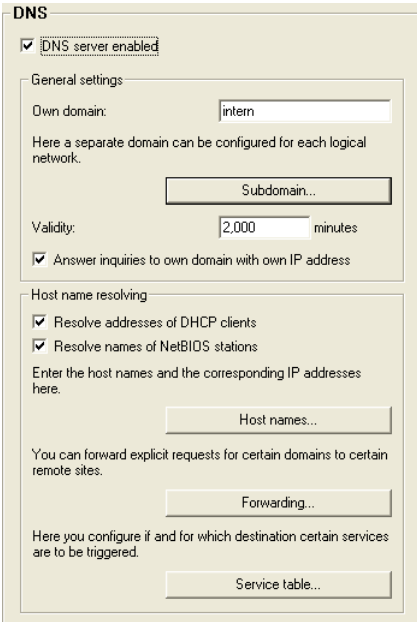
A DNS server translates the names of certain stations (e.g. www.company.com) to their IP addresses (e.g. 208.49.229.140). Normally, your Internet provider’s DNS server looks up the names of all Internet addresses. You can use the unit’s DNS server to translate the names of stations in your local network. Queries for names that are not known to the unit are automatically forwarded to your Internet provider's DNS server.

Configuring the DNS server is accomplished by enabling the DNS server, then making the following DNS settings:

- General settings
- Defining subdomains
- Host name resolution settings
- Creating host names
- Forwarding explicit requests
- Configuring services

To enable the DNS server:

☐ Navigate to the following dialog:`Configuration : IPv4 : DNS` and select the option "DNS server enabled".


DNS
DNS server enabled
General settings
Own domain:
intern
Here a separate domain can be configured for each logical network.
Subdomain...
Validity:
2,000
minutes
Answer inquiries to own domain with own IP address
Host name resolving
Resolve addresses of DHCP clients
Resolve names of NetBIOS stations
Enter the host names and the corresponding IP addresses here.
Host names...
You can forward explicit requests for certain domains to certain remote sites.
Forwarding...
Here you configure if and for which destination certain services are to be triggered.
Service table...

DNS settings can be entered via this dialog.

General DNS Settings

Enter values for the following general DNS settings in the ‘DNS’ dialog:

- Own domain:
  If you have an intranet of your own to which you would like to assign a domain name, enter it here (e.g. myhome.intern). If, for example, a computer with the name myhost were located in your network, its full name would be myhost.myhome.intern. However, you may also enter the name of your local network here if it belongs to a valid Internet domain (e.g. company.com).
- Validity:
  Some computers save the names and addresses of locations looked up by the DNS server to provide faster access to this information in the future. Enter the duration for which this stored data will remain valid. It will be necessary for the computer to request the information again after this period has elapsed.
- Answer inquiries to own domain with own IP address: (Self-explanatory).

Defining Subdomains

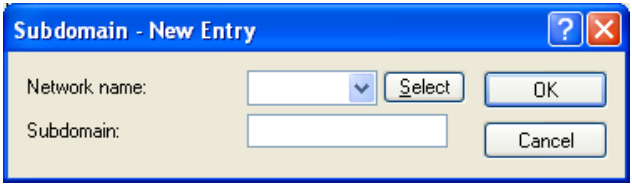
You can also define a separate sub-domain for each logical network. If, for example, your domain (own domain) is named 'internal' and the sub-domain of a logical network is named ‘intranet’, then the domain for this logical network would be intranet.internal. The name of a server in this network consists of:

hostname.subdomain.own-domain.

If your own domain is not specified, then define the desired domain for each logical network completely in the sub-domain. The domains defined here are distributed to the logical networks by the DHCP server in the device. To configure a subdomain:

☐ Beginning in the ‘DNS’ dialog, click ‘Subdomain...’.

☐ In the ‘Subdomain’ window, click ‘Add...’ to open the ‘New Entry’ dialog:



Configure the following parameters for each subdomain:

- Network name: The hostname.
- Subdomain:
  The name of the subdomain and, if appropriate, the own domain.

Hostname Resolution Settings

Enter values for the following hostname resolution settings in the ‘DNS’ dialog:

- Resolve address of DHCP clients:
  Select this to have the DNS server look up the names of stations that have requested an IP address via DHCP.
- Resolve names of NetBIOS stations:
  Select this to have the DNS server translate the names of stations that are known to the NetBIOS router.

Creating Host Names

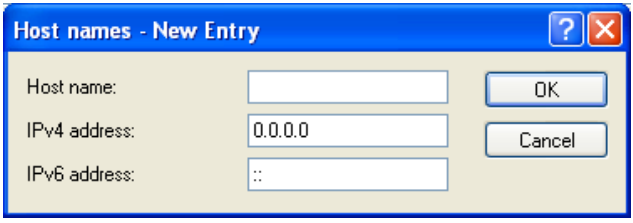
A client sends a query to the DNS server when it wants to have the name of a station looked up. The server responds to this query with the IP address entered here. You should create a list of host names, associating each entry with its respective IP address, including every client that meets all the following tests:

– the client hostname and IP address are known
– the client is located outside your own LAN
– the client is not on the Internet, and
– the client is accessible via the router

To enter a client to the host name list:

☐ Beginning in the ‘DNS’ dialog, click ‘Host names...’.

☐ In the ‘Host names’ window, click ‘Add...’ to open the ‘New Entry’ dialog:



Configure the following parameters for each host name entry:

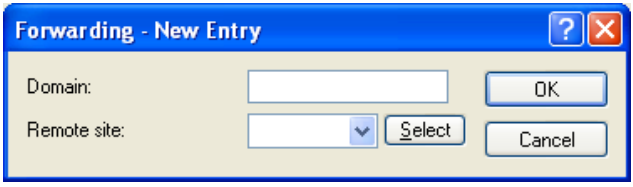
- Host name:
  Enter the name of the station here. For example, if you have a computer named myhost and the name of your domain is myhome.intern, then enter the host name myhost.myhome.intern.
- IPv4/IPv6 address: Enter the IP address of the station.

Forwarding Explicit Requests

To resolve entire name areas of another DNS server, you can add a forwarding entry consisting of a name area and remote station. When entering the name areas, you can use the wildcards '?' (for individual characters) and '*' (for multiple characters). To reroute all domains with the ending '.intern' to a DNS server in the LAN of the remote station 'COMPANY', create the following entry

☐ Beginning in the ‘DNS’ dialog, click ‘Forwarding...’.

☐ In the ‘Forwarding’ window, click ‘Add...’ to open the ‘New Entry’ dialog:



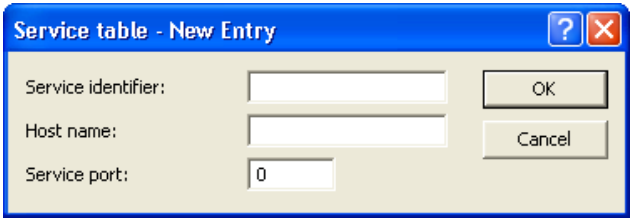
Configure the following parameters for each host name entry:

- Domain:
  Enter the name domain area. The entry `*.interal` for example causes all domains ending with '.intern' being redirected.
- Remote site:
  Enter the name of the remote station.

Configuring Services

☐ You can identify services to be resolved by the router.

☐ In the ‘Service table’, click ‘Add...’ to open the ‘New Entry’ dialog:



Configure the following parameters for each service to be resolved:

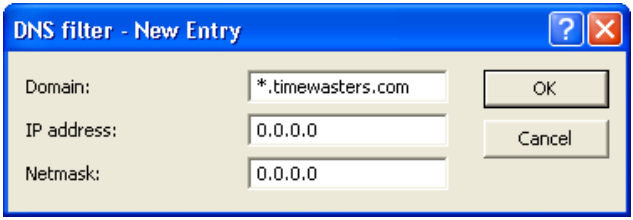
- Service identifier:
  Enter the service to be resolved according to RFC 2782.
- Host name:
  Enter the name of the host providing the specified service. If for example there is a computer named myhost and the name of your domain is myhome.intern, enter myhost.myhome.intern as the station name.
  – The station name '[self]' may be entered as name, if it is the device itself.
  – A dot '.' may be specified if this service is blocked and therefore not to be resolved. In this case the specification of a port number will be ignored.
- Service port:
  The port number used by the named service at the specified station.

14.3.4 URL Blocking

You can block access from your network to specific stations or domains with the filter list. To access the filter list:

☐ Navigate to the following dialog:`Configuration : IPv4 : DNS Filter` and click "DNS filter".

☐ In the ‘DNS filter’ list, click ‘Add...’ to open the ‘New Entry’ dialog:



To enter a new DNS filter item, complete these parameters:

- Domain:
  Enter the name of a destination station or domain that should be blocked from access. You can use the wildcards '?' for single characters and '*' for groups of characters, for example `*.mydomain.com`.
- IP address:
  Enter the IP address of a station, or range of stations, that are denied access to domain. A value of ‘0.0.0.0’ describes all computers in the network.
- Netmask:
  Enter the netmask of a station, or range of stations, that are denied access to domain. A value of ‘0.0.0.0’ describes all networks.
- IPv6 prefix:
  Specify the IPv6 prefix to be used by the device for filtering IPv6 addresses by domain. The value `::/0` describes all IPv6 addresses.

Note: The list in the DNS statistics contains the 64 most frequently requested names and provides a good basis for setting up the filter list. If your LAN uses subnetting, you can also apply filters to individual departments by carefully selecting the IP addresses and subnet masks.

14.3.5 Dynamic DNS

Systems with dynamic IP addresses become accessible over the WAN—for example over the Internet—via so-called Dynamic DNS service providers, e.g. www.dynDNS.org. Thereby a OpenBAT device becomes available under a certain DNS-resolvable name (FQDN – "fully qualified Domain Name," for example "http://MyDevice.dynDNS.org").

To accomplish maintenance for a remote site, for example, you just need to know the appropriate Dynamic DNS name.

Updating IP address entries in the Dynamic DNS server

Dynamic DNS providers support a set of client programs, which can determine the current assigned WAN IP address of a OpenBAT device via different methods (3, below), and transfer this address—in case of a change—to their respective Dynamic DNS server.

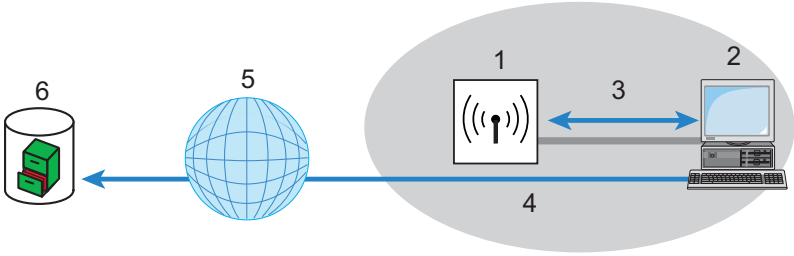
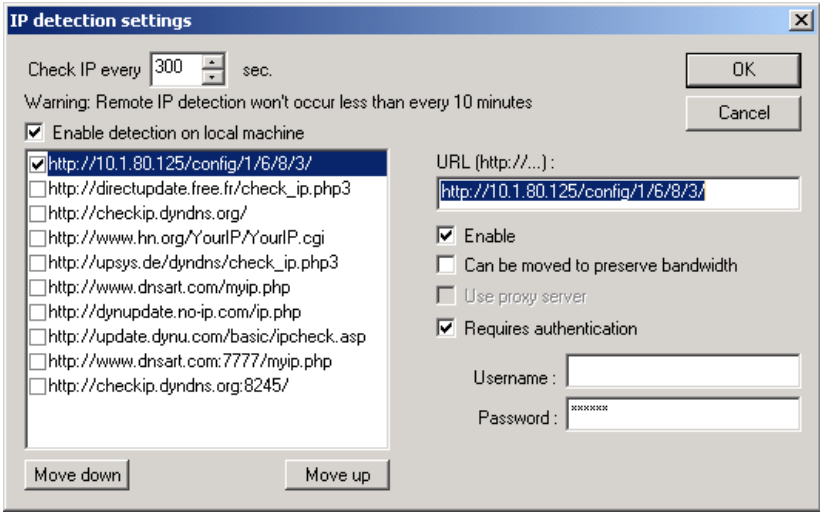


Figure 126:Updating the current IP address in the dynamic DNS server

1:OpenBAT device	4: PC updates DNS server
2: PC with DynDNS client program	5: Internet
3: PC determines current IP address of OpenBAT	6: Dynamic DNS server

The current WAN IP address of a device can be selected at:

```
http://<Address of the Device>/config/1/6/8/3/
```



Note: The above screenshot illustrates how to access the WAN IP address on the WEB interface from an external application.

Alternatively the OpenBAT device can directly transmit the present WAN IP to the DynDNS provider:

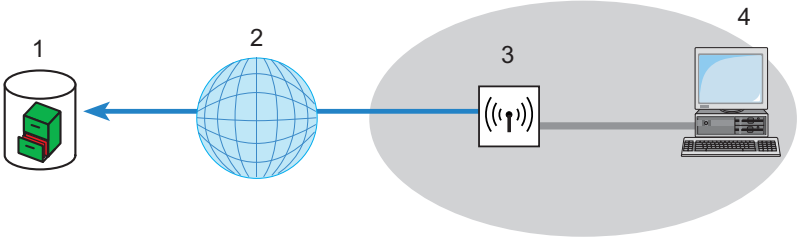
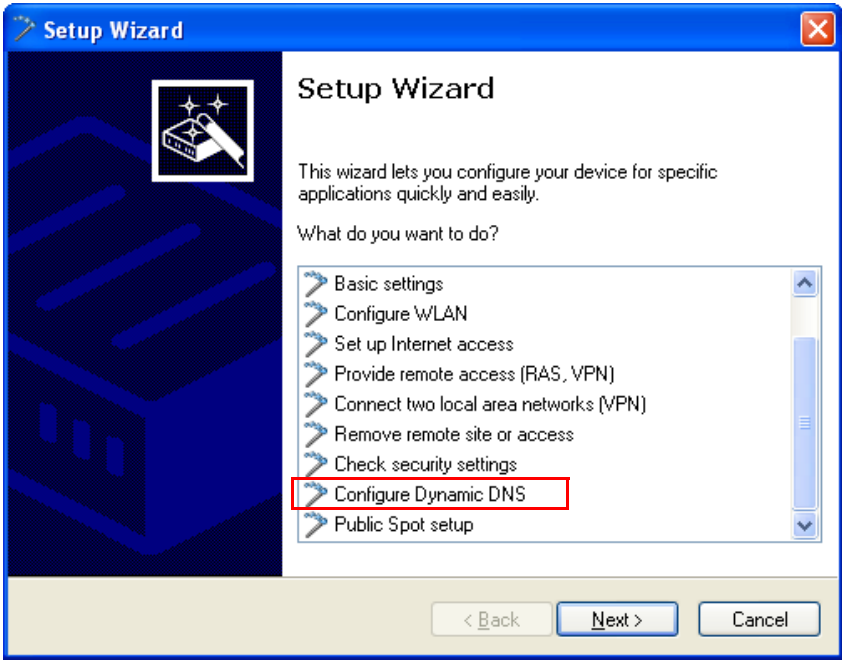


Figure 127:The OpenBAT device directly transmits its IP address to the DynDNS provider.

1: DynDNS provider	3: OpenBAT Device
2: Internet	4: Client

The settings necessary for this can be adjusted easily by using the ‘Configure Dynamic DNS’ Setup Wizard in LANconfig, see section "Configure Dynamic DNS":


Setup Wizard
Setup Wizard
This wizard lets you configure your device for specific applications quickly and easily.
What do you want to do?
Basic settings
Configure WLAN
Set up Internet access
Provide remote access (RAS, VPN)
Connect two local area networks (VPN)
Remove remote site or access
Check security settings
Configure Dynamic DNS
Public Spot setup
< Back
Next >
Cancel

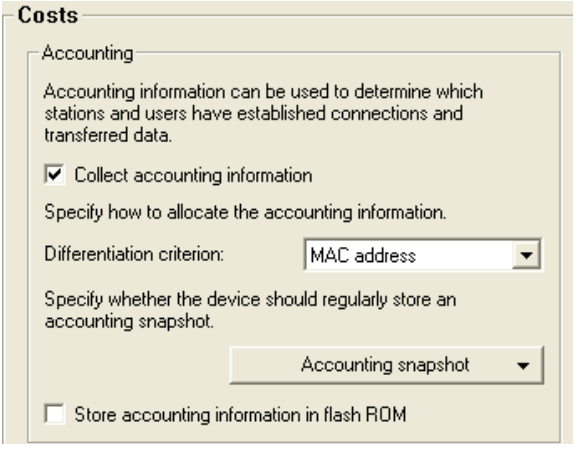
14.4 Accounting

Information on connections between clients in the local network and various remote stations is saved in the accounting table with entries for the connection time and the transferred data volume. Using accounting snapshots, accounting data can be regularly saved at specific times for later evaluation.

14.4.1 Configuring General Accounting Parameters

To configure general accounting parameters:

☐ Navigate to the following dialog:`Configuration : Management : Costs`.


Costs
Accounting
Accounting information can be used to determine which stations and users have established connections and transferred data.
Collect accounting information
Specify how to allocate the accounting information.
Differentiation criterion:
MAC address
Specify whether the device should regularly store an accounting snapshot.
Accounting snapshot
Store accounting information in flash ROM

Configure the following general accounting parameters:

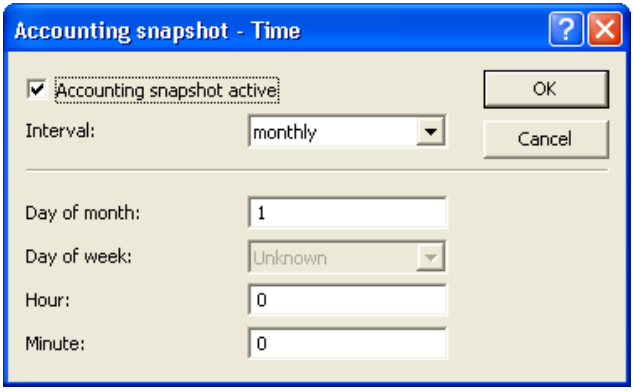
- Collect accounting information:
  Turns accounting on or off.
- Differentiation criterion:
  Select the feature according to which the accounting data are to be gathered:
  – MAC address: The data are collected according to the client's MAC address.
  – IP address: The data are collected according to the client's IP address.

  Note: When dynamic IP addresses are in use, the option 'IP address' can lead to inaccurate accounting data. In this case, it may not be possible to accurately assign the data to users. Conversely, with this setting, data can be separated from clients that are behind another router and therefore appear with the same MAC address as the router in the accounting list.
- Store accounting information in flash ROM:
  Turn accounting data in flash memory on or off. Accounting data saved to flash will be preserved in the event of a power outage.

14.4.2 Configuring the Snapshot

You can specify if and when the device should capture and store an accounting snapshot. To do this:

☐ In the ‘Accounting’ section of the ‘Costs’ dialog, click ‘Accounting snapshot’ and select the time menu item to open the ‘Time’ dialog:



In the ‘Time’ dialog, enter values for the following properties:

- Accounting snapshot active:
  Turns intermediate storage of accounting data on or off.
- Interval: Monthly, Weekly, Daily.
- Day of month:
  The day of the month on which caching will take place: Relevant if the interval is 'monthly'.
- Day of week:
  The weekday on which caching will take place. Relevant if the interval is 'weekly'.
- Hour: The hour on which caching will take place: 0 to 23
- Minute: The minute in which caching will take place: 0 to 59

14.5 Call Charge Management

The capability of the router to automatically establish connections to all desired remote sites, and to close them again when no longer required, provides users with extremely convenient access, e.g., to the Internet. However, very substantial costs can be incurred by data transfer over paid lines if the router is configured diffusely (e.g. in the filter configuration) or by excessive use of the communications opportunities (e.g. extended surfing in the Internet).

14.5.1 Connection limits for DSL and cable modem

Even though a DSL or cable modem connection behaves like a leased line, in that it is continuously online, connection charges can accrue over time, depending on the provider.

Note: Only DSL connections will be discussed in the remainder of this section The explanations apply equally well, however, to any other type of connection made via the Ethernet WAN port of the OpenBAT device, for example, cable modem connections.

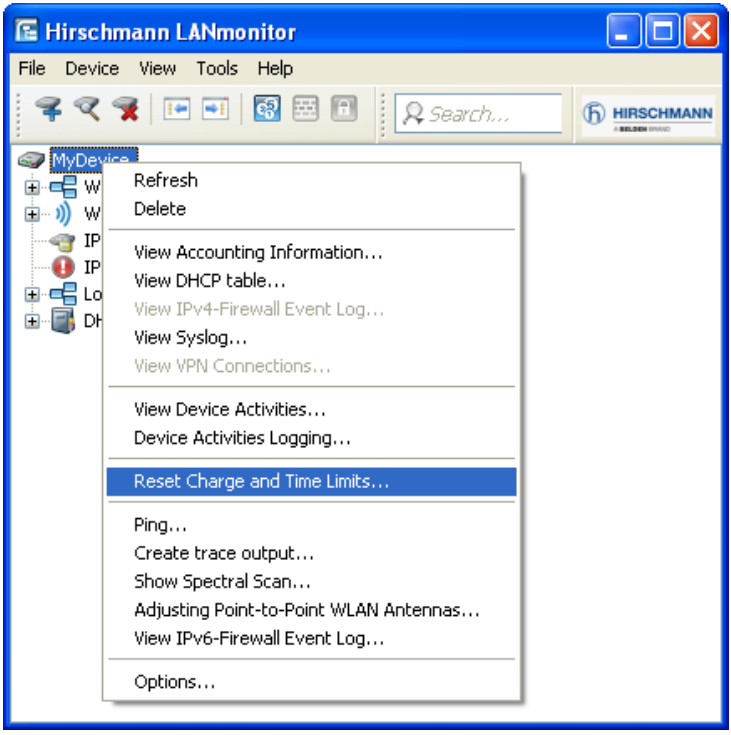
To limit the costs, a time limit for DSL connections can be set for a specified period of time. By default the DSL connections can be used for a maximum of 600 minutes in 6 days.

If the limit is reached, all DSL connections are automatically terminated. As soon as the current period has elapsed, the time count is reset and the connection enabled. The administrator can manually reset the time count and re-establish the connection before the connection is automatically re-enabled.

If the connection has a charge limit and a short hold of '0' or '9999' seconds, the charge control is switched off and the connection is kept open even if the limit is exceeded.

If in an exceptional case you would like to extend the online budget, e.g. to download a large file from the internet, you can manually reset the limit, as follows:

☐ In LANmonitor, select the device indicating a time event, click the right mouse button, then select '`Reset Charge and Time Limits...`' from the pop-up menu.



Note: If you cannot see the system information in LANmonitor, you can display it as follows:

☐ Select `View : Show Details : System Information`.

You can also access the commands to activate the additional time limit at:

`HiLCOS Menu Tree : Setup : Fees`

The additional time limit is activated for the current period, in the following period normal time limit is set.

14.6 Time Server

OpenBAT devices can obtain highly precise time information via publically accessible time servers in the Internet (NTP server with open access policy, e.g., that of the Physikalisch-Technische Bundesanstalt). The time obtained this way can be made available to all stations in the network.

14.6.1 Configuring the time server with LANconfig

To provide the current time in the local network your OpenBAT device has to regularly apply the time from a time server. Configuring a time server is a two-step process:

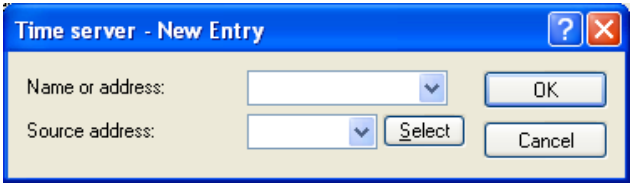
- Selecting a time server for the device
- Enabling the time server

Selecting a Time Server

You can create a list of available time servers in LANconfig. The OpenBAT device will attempt to obtain time information from time servers in the order in which they appear in the list. To enter a time server to this list, follow these steps:

☐ Navigate to the following dialog:`Configuration : Date & Time : Synchronization` and click "Time server".

☐ In the ‘Time server’ window, click ‘Add...’ to open the ‘New Entry’ dialog:



Define a new time server entry using the following parameters:

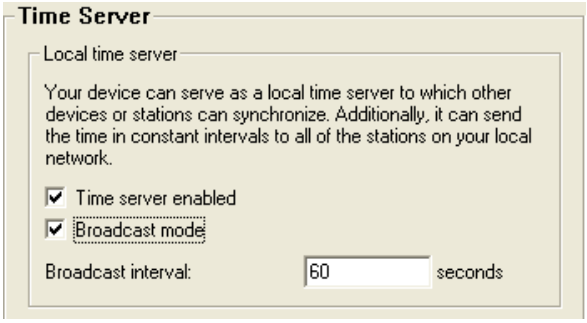
- Name or address:
  Select a time server from the list, or type in a time server using its name or IP address.
- Source IP address:
  An optional source address can be configured here. This address is used instead of the 'Name or address' setting, which is otherwise obtained automatically for the respective destination address.

After an item has been entered into the list, you can use the up/down buttons to change the position of a selected list item.

Enabling the Time Server

After one or more time server entries have been created, and their relative positions established in the list, you can enable the time service, as follows:

☐ Navigate to the following dialog:`Configuration : Date & Time : time server`.


Time Server
Local time server
Your device can serve as a local time server to which other devices or stations can synchronize. Additionally, it can send the time in constant intervals to all of the stations on your local network.
Time server enabled
Broadcast mode
Broadcast interval:
60
seconds

To enable the time service, configure the following parameters:

- Time server enabled:
  Enables the NTP time service.
- Broadcast mode:
  Select this to have the server broadcast the actual time to all reachable devices or stations in the local network in constant intervals.

14.6.2 Configuring the time server with WEBconfig

You can also use Telnet or WEBconfig to configure the time server, at:

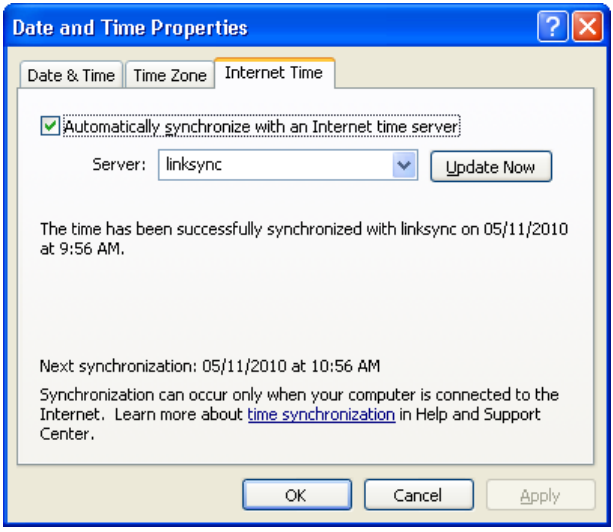
`HiLCOS Menu Tree : Setup : NTP`

14.6.3 Configuring NTP Clients

The NTP clients need to be configured so that they use the time information from the OpenBAT device. The Windows XP operating system provides an integrated NTP client; other operating systems may require installation of a separate NTP client. Linux distributions have to be installed with NTP.

You can open the settings for date and time in a Windows system as follows:

☐ Double click on the time setting on the Windows task bar, then select the ‘Internet time’ tab:

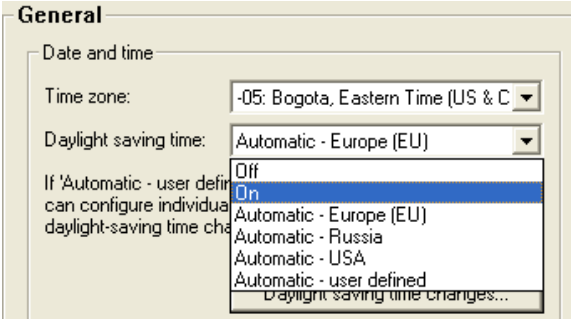

Date and Time Properties
Date & Time
Time Zone
Internet Time
Automatically synchronize with an Internet time server
Server:
linksync
Update Now
The time has been successfully synchronized with linksync on 05/11/2010 at 9:56 AM.
Next synchronization: 05/11/2010 at 10:56 AM
Synchronization can occur only when your computer is connected to the Internet. Learn more about time synchronization in Help and Support Center.
OK
Cancel
Apply

Configuring Time

OpenBAT devices work internally with coordinated world time (UTC). For protocol displays and time-related settings (e.g. cron jobs), the local time is derived from the selected time zone. To take local daylight-saving time into account, settings can be configured according to local conditions.

To configure the time for a device:

☐ Navigate to the following dialog:`Configuration : Date & Time : General`.



Configure the following parameters:

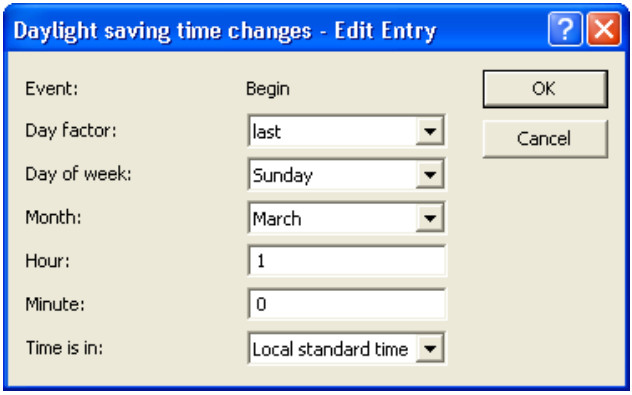
- Time zone:
  Select your time zone.
- Daylight saving time:
  Values include:
  - Off: The system time will not be adjusted to daylight-saving time.
  - On: One hour is added statically to the current system time (comprised of UTC and time zone).
  - Automatic (EU, USA, Russia): The daylight-saving time change is performed automatically in conformance with the time zone of the device's location.
  - Automatic (user-defined): If the device is located in an area that is not listed here, then the daylight-saving time change options can be manually defined by the user.

User-Defined Daylight Savings Time Settings

User-defined values can be set for the beginning and the end of the automatic daylight-saving time change.

☐ Open the `Configuration : Date & Time : General` and click "Daylight saving time changes".

☐ In the ‘Daylight saving time changes’ window, select the ‘Begin’ event and click ‘Edit...’:



Configure the following parameters: for the beginning of the daylight saving time period.

- Day Factor:
  Defines the recurring weekday of the month when the change will take place.
- Day of the Week: The day of the week the change begins.
- Month: The month the change begins.
- Hour: The hour the change begins.
- Minute: The minute the change begins.
- Time is in:
  Defines the time zone which is the basis for the time settings in this table (Coordinated Universal Time or Local Standard Time).

Next, select the ‘End’ entry in the ‘Daylight Saving time changes’ table, click ‘Edit...’ and configure the same parameters defining the end of the daylight savings time period.

14.7 Scheduled Events

This function is intended to allow the device to execute predefined commands in a telnet-like environment, at times defined by the user. The functionality is equivalent to the UNIX cron service. Any desired OpenBAT device command line function can be executed. Thus, the full feature set of all OpenBAT devices can be controlled by this timing function. The following examples illustrate the scheduled events function:

- A scheduled connection:
  Many leased lines disconnect automatically after 24 hours of continuous operation. This enforced disconnection can have some unwanted side-effects, for example if it occurs at an inconvenient time. To control the disconnecting time, a manual disconnection can be set, thereby avoiding ill-timed disconnections.
- Time-dependant firewall or QoS rules:
  Firewall and QoS rules are, at first, constant in their duration. However, it can be useful to apply variable settings for different times or days. For example: for off-hours or weekends may require different levels of bandwidth availability than during business hours.
- Regular firmware or configuration updates:
  Time-controlled rules let you toggle the settings of particular parameters, and switch to an entirely different configuration. This possibility allows you to pool a whole string of settings and change them all at once with a single command. Thus, you can apply one set of operating settings to the device over the weekend, then switch back to a different configuration on Monday mornings, with just one command. In addition, a regular update of the newest firmware from a single source is adjustable.
- E-mail messages:
  With time-controlled rules, you can configure the OpenBAT device to send e-mail notification to the administrator for specific firewall events, and also at scheduled times. A scheduled e-mail might contain information about successfully re-establishing an internet connection after an enforced disconnection, or a re-boot of the device after a restart.

- Time-dependent interfaces:
  The time dependant use of interfaces for a set duration can also be configured using time-controlled rules. For example, a WLAN interface can permit the wireless access to the network exclusively at certain times.
- Deleting specific tables:
  It can be useful to regularly clear the content of some tables in the OpenBAT device operating system. For example, if your Internet access has a monthly limited transfer volume, you can delete your accounting table monthly to contain a survey of just the present transferred data volume.

14.7.1 CRON Jobs With Time Delay

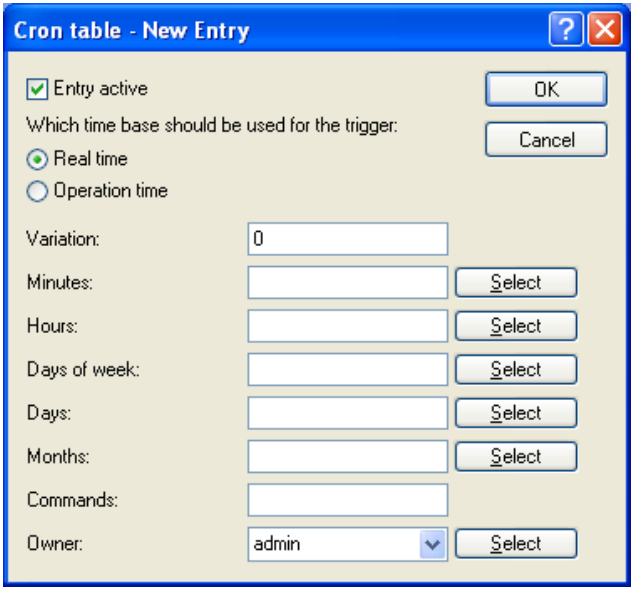
CRON jobs are used to automatically carry out recurring tasks on a OpenBAT device at specified times. If the installation features a large number of active devices, all of which are subjected to the same CRON job at the same time (e.g. updating a configuration by script), unpleasant side effects can result: All devices may simultaneously attempt to establish a connection, for example. To avoid these effects, CRON jobs can be set with a random delay time between 0 and 59 minutes.

14.7.2 Configuring a CRON Job

You can use LANconfig to configure a CRON job, as follows:

☐ Navigate to the following dialog:`Configuration : Date & Time : General` and click "Cron table".

☐ In the ‘Cron table’ window, click ‘Add...’ to open the ‘New Entry’ dialog:



Enter values for the following CRON job properties:

- Entry active: Activates or de-activates the CRON job entry.
- Which time base should be used for the trigger:
  This field determines whether time control is based on real time or on the device's operating time:
  – Real time: These rules evaluate all time/date information.
  – Operation time: These rules exclusively evaluate the minutes and hours since the last time the device was started.
- Variation:
  This specifies the maximum delay, from 0 to 65536 minutes, for the start of the CRON job after the set start time. The actual delay time is determined randomly and lies between 0 and the time entered here.
- Minutes:
  Enter a comma-separated list of those minutes for which you want the specified device commands to be executed. If all other specified time fields match, the associated device commands will be executed once for every minute specified.

- Hours:
  Enter a comma-separated list of those hours for which you want the specified device commands to be executed. If all other specified time fields match, the associated device commands will be executed once for every hour specified.
- Days of week:
  Use a comma-separated list to enter the days of the week on which you want the specified device commands to be executed. The days of the week are sequentially represented by numbers:
  – 0 = Sunday
  – ...
  – 7 = Saturday
- Days:
  Use a comma-separated list to enter all of the days of a month on which you want the specified device commands to be executed. If all other specified time fields match, the associated device commands will be executed on every day of month specified (can be refined optionally by stating specific hours and minutes).
- Months:
  Use a comma-separated list to enter all of the months of a year on which you want the specified device commands to be executed. If all other specified time fields match, the associated device commands will be executed in every specified month (can be refined optionally by stating specific days, days of week, hours and minutes).
- Commands:
  Use a semicolon separated list to enter all commands that you want to be executed if all time entries match. Any commands that you can enter in a Telnet session are allowed. Advisable commands are those that end in an action, e.g. PING, TESTMAIL, DO or SET.
- Owner:
  An administrator defined in the device can be designated as owner of the CRON job. If an owner is defined, then the CRON job commands will be executed with the rights of the owner.

Real-time based rules can be executed provided that the device has a time from a relevant source, e.g. via NTP. For example:

time base	min.	hours	w-days	m-days	months	Command
Real time	0	4	0/-6	1/-31	1/-12	do /oth/man/disconnect internet
Real time	59	3	0/-6	1/-31	1/-12	mailto:admin@mydevice.de?subject=disconnection?body=Manual disconnection of the internet connection
Real time	0	0	–	1	–	do /setup/accounting/delete
Real time	0	18	1.2, 3.4, or 5	–	–	do /oth/man/connect HEADQUARTER

- The first entry cuts the connection to the internet provider every morning at 4 am (forced disconnection).
- The second entry sends an information mail every morning at 3:59 am (directly before the forced disconnection) to the admin.
- The third entry deletes on the first of every month the accounting table.
- The fourth entry builds up a connection to the headquarter every week day at 6 pm.

Note: Time-based rules are performed with an exactness of one minute. Keep in mind that the language of the commands should be the same as the language of the console, otherwise the commands will be ignored. The default language is English, but can be changed.

14.8 RADIUS

The Remote Authentication Dial-In User Service (RADIUS) is referred to as a ‘triple-A’ protocol. The three ‘A’s stand for:

- Authentication
- Authorization
- Accounting

RADIUS enables you to grant users access to a network, to assign them specified rights, and to track their actions. Where necessary, the RADIUS server can also be used in the billing of user services such as WLAN hot spots. For every action performed by the user, the RADIUS server can run an authorization procedure releasing or blocking access to network resources on a per user basis.

RADIUS requires three different devices for its operation:

- Client: This is a device (PC, notebook etc.) from which the user wishes to dial in to the network.
- Authenticator: A network component positioned between network and client and which forwards on the authorization. This task can be performed by a OpenBAT Access Point, for example. The authenticator is referred to as the Network Access Server (NAS).

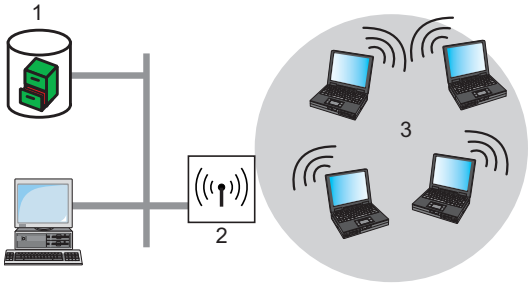


Figure 128:Remote Authentication Dial-in User Service

1: RADIUS Server
2: Authenticator
3: Clients

- Authentication server: A RADIUS server on which user data is configured. This is usually located within the same network for which it issues access authorizations. It is accessible to the client via the authenticator. Some scenarios may also allow the use of a OpenBAT access point for this task.

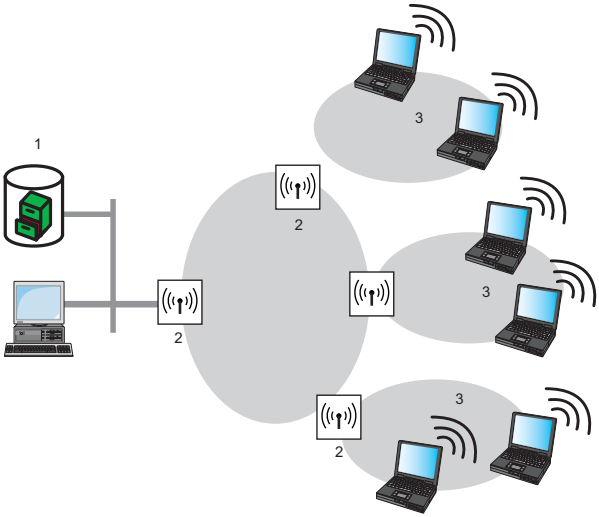


Figure 129:Authentication server

1: RADIUS Server
2: Authenticator
3: Clients

The authenticator has no initial information about the clients that want to register. This information is stored in a database on the RADIUS server. The registration information the RADIUS server needs for the authentication process is stored in the database, and can vary from network to network. The authenticator has just the one task: to transfer authentication information between the client and the RADIUS server. Access to a RADIUS server can be configured in several ways:

- Using PPP when dialing into a network (see on page 905).
- Via WLAN (see on page 908).
- Via the 802.1x protocol (see on page 910).

14.8.1 How RADIUS Works

The authentication process of a client using the RADIUS server authenticator can vary in complexity, depending on the implementation. In a simplified application, the client sends its registration data to the RADIUS server via the authenticator and receives back either an ‘Accept’ or a ‘Reject’ message.

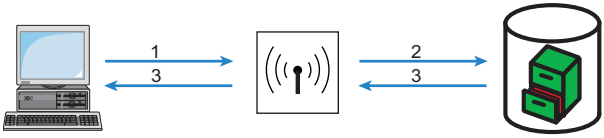


Figure 130:Simplified RADIUS application

1: User ID
2: User ID
3: Accept message

In more complicated applications, the RADIUS server can request additional registration data using what is known as a ‘Challenge’. The handshake sequence looks something like this:

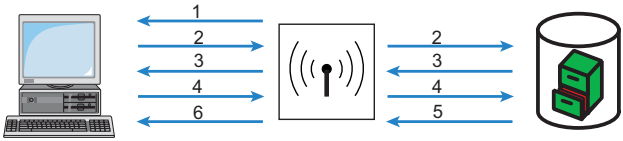


Figure 131:More complicated RADIUS application

1: Identity	4: Login data
2: User ID	5: Global key
3: Challenge	6: Session key

14.8.2 Configuring RADIUS as Authenticator or NAS

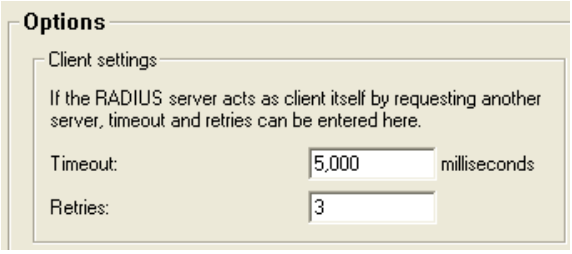
The RADIUS protocol is supported by OpenBAT devices in various application cases. For each of these cases, there is a specific set of parameters that can be configured independently of other applications. There are also general parameters that need to be configured for each of these applications. Some devices support all applications.

General Settings

General settings apply to all RADIUS client applications. Default values have been selected such that they need not usually be changed.

Perform the following steps to configure the OpenBAT device for dial-in via PPP in such a manner that the access authorization of the clients can be checked by RADIUS.

☐ Navigate to the following dialog:`Configuration : RADIUS Server : Options`.



Enter settings for the following parameters:

- Timeout:
  The number of milliseconds to wait before the next authentication attempt. Default = 5000.

  Note: With PPP authentication using RADIUS, the device dialing accepts the RADIUS timeout configured here.

- Retries:
  The number of attempts before the request is interpreted as rejected. Default = 3.

RADIUS Accounting

Accounting for a logical WLAN network can be enabled from a RADIUS server by enabling the ‘RADIUS Accounting’ option in the logical WLAN settings for the network. This can be performed at the following location:

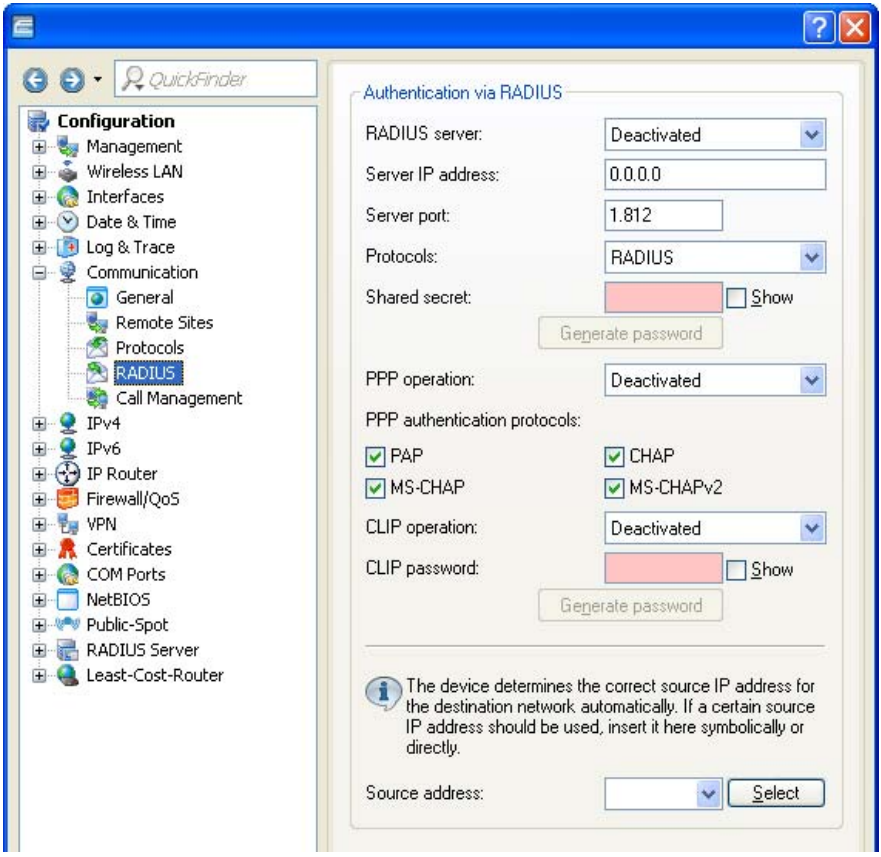
`HiLCOS Menu Tree : Setup : Interfaces : WLAN Network`

Access Checking Via PPP and RADIUS

When a client seeks to gain access using the point-to-point protocol (PPP), RADIUS can be used to check client authorizations. A client can dial in to the network from anywhere. The resulting data transmission between client and authenticator is encrypted.

Perform the following steps to configure the OpenBAT device for dial-in via PPP in such a manner that the access authorization of the clients can be checked by RADIUS.

☐ Navigate to the following dialog:`Configuration : Communication : RADIUS`.



Enter settings for the following parameters:

- RADIUS server:
  When authenticating using RADIUS, the user administration and authentication tasks are passed on to a RADIUS server. Values include:
  - Deactivated: The functionality of RADIUS is disabled and no requests are forwarded to the RADIUS server.
  - Activated: The functionality of RADIUS is enabled and requests may be forwarded to the configured RADIUS server. Depending on the setting, other sources may be used for the authentication process (e.g. PPP list).
  - Exclusive: RADIUS functionality is enabled and the authentication process is run exclusively by RADIUS.
- Server IP address:
  The IP address of your RADIUS server from which users are managed centrally.
- Server port:
  The port used for communication to your RADIUS server.
- Protocols: Select ‘RADIUS”.
- Shared secret:
  The key to be used for coding data. The key also needs to be configured on the RADIUS server.

- PPP operation:
  A RADIUS server may be used for the authentication process when dialing-in using PPP. Settings include:
  - Deactivated: PPP clients are not authenticated using RADIUS. They are checked exclusively using the PPP list.
  - Activated: RADIUS authentication for PPP clients is enabled. User data supplied by clients is first checked using the PPP list. If no matching entry is found in the PPP list, the client is checked by the RADIUS server. Authentication is successful if the PPP list check or RADIUS server check returns as positive.
  - Exclusive: RADIUS authentication for PPP clients is enabled. User data supplied by clients is checked exclusively by the RADIUS server. In this mode, it is just the advanced settings of the PPP list for the user which are interpreted (e.g. check for PAP/CHAP – or the allowed protocols IP, IPX and/or NetBIOS).
- PPP authentication protocols:
  The security measures which apply when authenticating a remote station.
- CLIOP operation:
  A RADIUS server may be used for control of a return call when dialing-in using PPP. The possible settings are:
  - Deactivated: The return call function is not controlled by RADIUS. An entry needs to appear in the name list to be used.
  - Activated: The RADIUS function for the return call is enabled. Telephone numbers reported by clients are first checked using the name list. If no matching entry is found in the name list, the telephone number is checked by the RADIUS server. If the name list check or RADIUS server check returns as positive, a return call can be established. If the telephone number communicated is in the name list, but no return call is active there, RADIUS ceases checking.
  - Exclusive: The RADIUS function for the return call is enabled. User data reported by clients is checked exclusively by the RADIUS server.

  In order to use the return call control from RADIUS, set up a user on the RADIUS server for each telephone number to be authenticated. The user name corresponds to the telephone number and the user password is the CLIP password specified here.

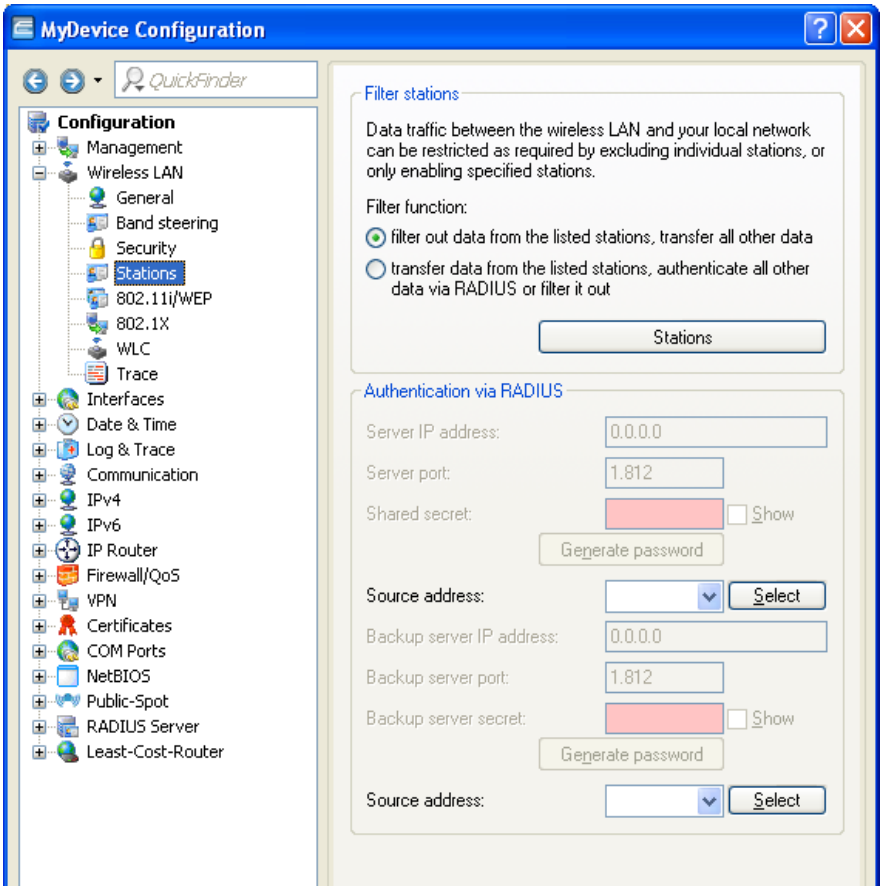
- CLIP password:
  Password for return call control. The generic values for retry and timeout also need to be configured. They are under PPP on the same screen as PPP parameters.
- Source IP address:
  An optional source address can be configured here. This address is used instead of the source address, which is otherwise obtained automatically for the respective destination address.

Access Checking via WLAN and RADIUS

When using a RADIUS server for the authentication of WLAN clients, the RADIUS server uses the MAC address to check client authorizations.

Perform the following steps to configure the OpenBAT device for dial-in via PPP in such a manner that the access authorization of the clients can be checked by RADIUS.

☐ Navigate to the following dialog:`Configuration : Wireless LAN :Stations`.



Enter settings for the following parameters:

- Filter function:
  Select the option ‘transfer data from the listed stations, authenticate all other via RADIUS or filter it out’.
- Server IP address:
  The IP address of your RADIUS server from which users are managed centrally.
- Server port:
  The port used for communication to your RADIUS server.
- Shared secret:
  The key to be used for coding data. The key also needs to be configured on the RADIUS server.
- Source IP address:
  An optional source address can be configured here. This address is used instead of the server IP address, which is otherwise obtained automatically for the respective destination address.
- Backup server IP address:
  The IP backup address of your RADIUS server from which users are managed centrally.
- Backup server port:
  The backup port used for communication to your RADIUS server.
- Backup shared secret:
  The backup key to be used for coding data. The key also needs to be configured on the RADIUS server.
- Source IP address:
  An optional source address can be configured here. This address is used instead of the source address, which is otherwise obtained automatically for the respective destination address.

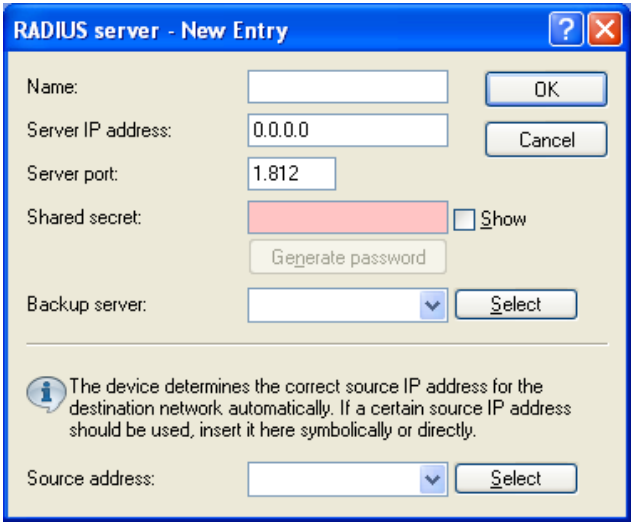
Access Checking via 802.1x and RADIUS

WLAN clients can use the 802.1x protocol for network registration. The OpenBAT device in access point mode can use this protocol to forward the log-ins to the RADIUS server. The MAC address is used for user identification.

To configure a public spot to forward data to one or more RADIUS servers:

☐ Navigate to the following dialog:`Configuration : Wireless LAN : IEEE 802.1x` and click "RADIUS server".

☐ In the ‘RADIUS server’ list, click ‘Add...’ to open the following dialog:



Enter settings for the following parameters:

- Name:
  In this table, each RADIUS server needs a unique name. The name 'DEFAULT' is reserved for WLAN networks that use an authentication process in line with IEEE 802.1x and that have not specified their own RADIUS server.

  By using the name defined in the "Key 1/passphrase" field, each WLAN network using authentication in line with IEEE 802.1x can be assigned its own RADIUS server
- Server IP address:
  The IP address of your RADIUS server from which users are managed centrally.
- Server port:
  The port used for communication to your RADIUS server.

- Shared secret:
  The the key to be used for coding data. Configure the key also on the RADIUS server.
- Backup server:
  Name of the backup server from the list of RADIUS servers configured so far.
- Source IP address:
  An optional source address can be configured here. This address is used instead of the server IP address, which is otherwise obtained automatically for the respective destination address.

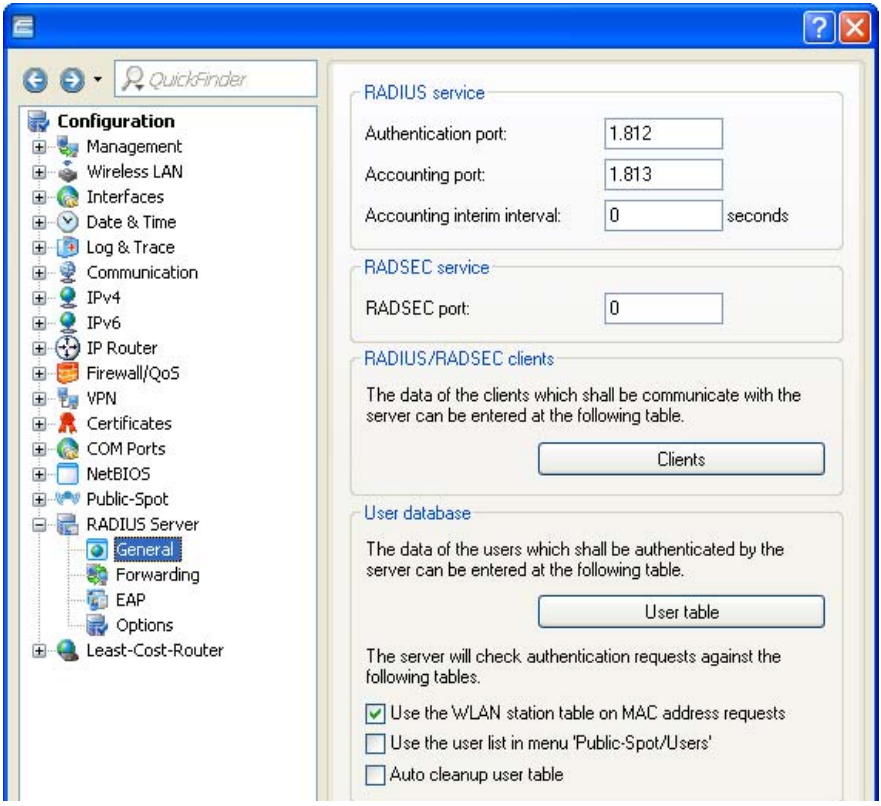
14.8.3 Configuring the RADIUS Server

In addition to its function as RADIUS authenticator or NAS, a OpenBAT device access point can also operate as a RADIUS server. When operating in this mode, information in the device on users authorized to register is made available to other access points operating in RADIUS authenticator mode.

General Settings

To configure the RADIUS Server, define the authenticator that may access the RADIUS server, the passphrase it needs for this access and the open port through which it can communicate with the RADIUS server. The authentication port applies globally to all authenticator instances. To enter general RADIUS server settings, do the following:

☐ Navigate to the following dialog:`Configuration : RADIUS Server : General`.



Enter settings for the following parameters:

- Authentication port:
  The TCP port used by the authenticators to communicate with the RADIUS server in the OpenBAT access point. Port '1812' is normally used. Port '0' disables the RADIUS server.
- Accounting port:
  The RADIUS server TCP port for receiving accounting information. Port '1813' is normally used.
- Accounting interim interval:
  The update frequency (in seconds) of accounting data sent to the RADIUS server.
- RADSEC port:
  The TCP port for transferring RADSEC encrypted accounting- or authentication requests to the server. Port '2083' is normally used. Port '0' deactivates the RADSEC service (see on page 927).
- Use the WLAN station table on MAC address requests:
  Self-explanatory.
- Use the user list in menu 'Public-Spot/Users':
  Compatibility setting for the Public Spot module. If you enable this setting, the RADIUS server also refers to the Public Spot's internal user list.

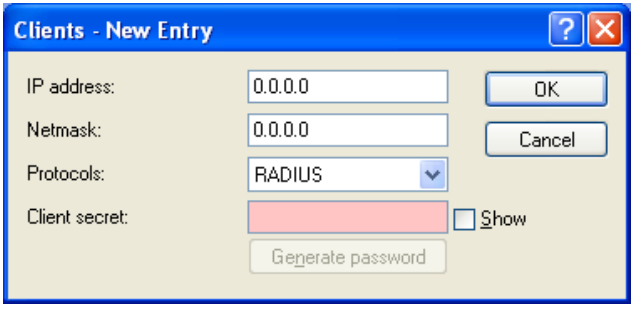
  Note: During technical development, this list was replaced as of HiLCOS 7.70 by the user administration via RADIUS. Also see the information in the chapter on creating Public Spot users (see page 309).
- Auto cleanup user table:
  Expired user accounts will be deleted automatically if this option is enabled. Auto cleanup will work both for accounts with either absolute or relative expiry. Relative account expiry and time or volume budgets work provided that the device is both the authentication and the accounting server.

Adding Clients

The client table can contain up to 16 clients that can communicate with the RADIUS server. To add clients:

☐ Navigate to the following dialog:`Configuration : RADIUS Server : General` and click "Clients".

☐ In the ‘Clients’ window, click ‘Add...’ to open the ‘New Entry’ dialog:



For each new RADIUS client, configure the following parameters:

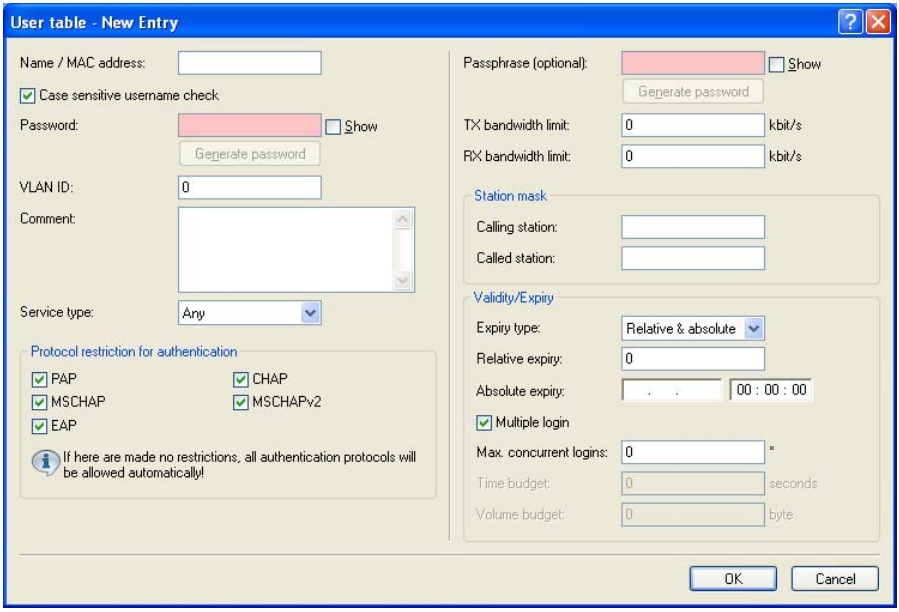
- IP address:
  The IP network—i.e., the range of client IP addresses—to which the defined password applies.
- Netmask: The IP network mask of the clients.
- Protocols:
  Select the protocol to be used to communicate between the RADIUS server and clients: RADIUS, RADSEC, or All.
- Client secret: The client password.

Adding Users

Up to 64 users can be entered into the user table, and these can be authenticated by the RADIUS server without reference to other databases. This user table is used for local requests to the RADIUS server, i.e. for requests with user name but no realm. To add users:

☐ Navigate to the following dialog:`Configuration : RADIUS Server : General` and click "User table".

☐ In the ‘User table’, click ‘Add...’ to open the ‘New Entry’ dialog:



For each new RADDIUS client, configure the following parameters:

- Name / MAC address:
  The user name.
- Please note that the user name is case-sensitive:
  You can specify whether the RADIUS server should carry out a case-sensitive user name check.
- Password:
  The user password.
- VLAN ID:
  Using this option, each user can be assigned a specific VLAN ID on successful authentication. The value '0' indicates no VLAN ID will be assigned.
- Comment:
  Here you can enter an arbitrary comment.
- Service type: The types of service this account may be used for:
  – Any
  – Framed

– Login
– Authorization only

Depending on the device, the number of entries with ‘Any’ or’ Login’ service type may be limited.

- Protocol restriction for authentication:
  Select one or more authentication methods to be applied to the user. If you do not select a restriction, all methods are allowed automatically.
- Passphrase:
  You can optionally specify a custom passphrase with at least 8 characters for any physical (MAC) address used in networks secured using 802.11i/WPA/AES-PSK.
  If no custom passphrase is specified, the device authenticates this MAC address with the passphrase stored for each logical WLAN under `Configuration: Management : 802.11i/WEP`.

  Note: This field has no significance for networks secured by WEP.
- TX bandwidth limit:
  To restrict the uplink for the corresponding user account, enter a value larger than `0` here. The value `0` stands for "unlimited".
- RX bandwidth limit:
  To restrict the downlink for the corresponding user account, enter a value larger than `0` here. The value `0` stands for "unlimited".
- Calling station mask:
  This mask restricts entries to particular IDs that are transmitted by the calling station (WLAN client). On authentication via 802.1x the MAC address of the calling station is provided in ASCII format (in capital letters), where character pairs are divided by hyphens (e.g. '00-10-A4-23-19-C0'). Using an * as placeholder, whole groups of IDs can be defined (e.g. '00-10-A4-*').
- Called station mask:
  This mask restricts entries to particular IDs that are transmitted by the called station (BSSID and SSID of the access point). On authentication via 802.1x MAC addresses of the called stations are transmitted in ASCII format (in capital letters), where character pairs are divided by hyphens. The SSID is added following a colon as separation mark (e.g. '00-10-A4-23-19-C0:AP1'). Using an * as

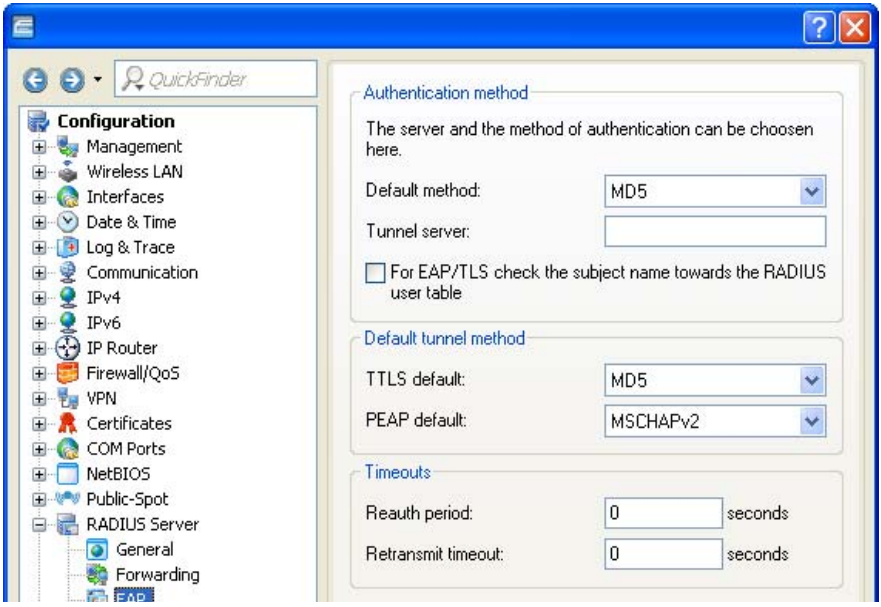
placeholder whole groups of IDs can be collected and defined as a mask. For example, the mask '*:AP1' defines an entry which applies for a client in the radio cell which is named 'AP1', independent from the access point it is registered to. Thus, the client can roam from one access point to another, keeping its authentication data.

- Expiry type:
  A point in time when validity of this account shall end. There are two types of limited validity, which may be selected independently, or together:
  – Relative: The validity of the account ends at a set amount of time after the first successful login.
  – Absolute: The validity of the account ends at a fixed point in time.
  – Never: The validity of the account does not end.
- Relative expiry:
  The relative amount of time, in seconds, until the account expires.
- Absolute expiry:
  The specific time and date when the account expires.
- Multiple login:
  Select this to permit more than one parallel session with the same user ID. If de-selected, the device rejects an authentication request for the given user ID if there is an ongoing session in the active session accounting table for this user. De-selecting this option is often a prerequisite for a reasonable enforcement of time and volume budgets.
- Max. concurrent logins:
  If multiple login is enabled, this field is used to specify the maximum number of parallel sessions allowed. The value `0` stands for "unlimited".
- Time budget:
  This setting set a maximum amount of time (in seconds) that may be consumed via this user account before access is denied. The time budget setting should be used exclusively if the device is both the authentication server and the accounting server. This selection is available on if Multiple login is de-selected.
- Volume budget:
  The maximum amount of bytes that may be transmitted by this user account before access is denied. This selection is available on if Multiple login is de-selected.

EAP Authentication

EAP operates as a framework for various authentication methods. Authentication methods cannot be suppressed. The EAP supplicant and the RADIUS server negotiate the EAP method with the standard EAP mechanism. Clients requesting a non-EAP method will be rejected by the RADIUS server. To configure EAP:

☐ Navigate to the following dialog:`Configuration : RADIUS Server : EAP`.



For each new RADIUS client, configure the following parameters:

- Default method:
  Select the method by which the RADIUS server should offer a client outside a TTLS/PEAP tunnel:
  - MD5: Defined in RFC 2284, EAP/MD5 is a simple challenge/ response protocol. It does not cater for mutual authentication nor does it offer a dynamic key such as those required for 802.1x authentication in wireless networks (WLANs). Thus it is used exclusively for the authentication of non-wireless clients or as a tunneled method as a part of TTLS.
  - GTC: (generic token card) Defined in RFC 2284 and RFC 3748, this protocol employs a text challenge from the authentication server, and a security token reply. Provides for the use of a one-time password.
  - MSCHAPv2: Defined in draft-kamath-pppext-eap-mschapv2-01.txt. As opposed to EAD/MD5, EAP/MSCHAPv2 supports mutual authentication but does not support dynamic keys, making it just as prone to dictionary attacks as EAP/MD5. This method is usually used within PEAP tunnels.
  - TLS: Defined in RFC2716. The use of EAP/TLS requires the use of a root certificate, a device certificate and a private key in the device. EAP/TLS provides enhanced security and the dynamic keys necessary for wireless connections; its implementation is complex, however, because each individual client requires a certificate and a private key.
  - TTLS,: Defined in draft-ietf-pppext-eap-ttls-05.txt. TTLS is based on TLS; it ignores client certificates and it utilizes the existing TLS tunnel to authenticate the client. The RADIUS server supports the following TTLS methods: PAP, CHAP, MSCHAP, MSCHAPv2, and EAP.
  - PEAP: Defined in draft-kamath-pppext-peapv0-00.txt. Similar to TTLS, PEAP is based on TLS and works with an EAP negotiation inside the TLS tunnel.

- Tunnel server:
  To handle tunneled EAP requests for TTLS and PEAP, enter an account listed in the forwarding table. Select a realm that does not conflict with other used realms. If left empty, the local RADIUS server forwards requests to itself, meaning that both the outer and inner EAP phases are handled by the local RADIUS server.
- For EAP/TLS check the subject name towards thr RADIUS user table:
  For TLS, the client only uses its certificate for authentication. If this is selected, the RADIUS server additionally checks to see if the certificate username is enclosed in the RADIUS user table.
- TTLS default / PEAP default:
  When using TLS or PEAP, two authentication methods are negotiated. Initially, a secure TLS tunnel is negotiated via EAP. Within this tunnel, a second authentication method is negotiated. In this negotiation, the server respectively offers a method to be accepted (ACK) or rejected (NAK) by the client. If the client rejects, it sends a proposal containing a method which it would prefer to use. If the suggested method is allowed by the server, it will be used. Otherwise the negotiation is aborted by the server. This parameter sets the method to be offered by the server for authenticating clients within TLS tunnels.
- Reauth period:
  If the internal RADIUS server answers CHALLENGE to a client request (authentication method negotiation not yet finished), the RADIUS server can notify the authenticator, how long (in seconds) it has to wait for a client answer before CHALLENGE will be sent anew. Value '0' deactivates the timeout for the authenticator.
- Retransmit timeout:
  If the internal RADIUS server answers ACCEPT to a client request (authentication method negotiation successfully finished), the RADIUS server can notify the authenticator, after which time (in seconds) it should do a re-authentication of the client. Value '0' deactivates the timeout for the authenticator.

RADIUS Forwarding

In the case of multi-layer EAP protocols such as TTLS or PEAP, the actual internal authentication can be carried out by a separate RADIUS server. Thus, an existing RADIUS server can continue to be operated to provide user tables, even though it is not EAP(/TLS) capable itself. In this situation the TLS/TTLS/PEAP tunnel is managed from the RADIUS server. The configuration of multi-layer protocols of this type is an element of a general method for the forwarding of RADIUS requests, whereby a RADIUS server can also be used as a RADIUS proxy. The concept of 'realms' is the basis for request forwarding and the proxy function. A realm is a character string which defines the validity of a range of user accounts. Once defined, the realm is a suffix to the user name separated by an @ character as follows:

user@realm

The realm can be seen as a pointer to the RADIUS server where the user account is managed. The realm is removed from the string prior to the search of the RADIUS server's user table. Realms allow entire networks which are mutually trustworthy to work with common RADIUS servers located in partner networks, and to authenticate users who move between these networks. The RADIUS server stores any connected RADIUS servers along with their associated realms in a forwarding table. The realm is searched for in this table in connection with the communicated user name. If no entry is found, the request is answered with an access reject. An empty realm is treated as a local request, i.e. the RADIUS server searches its own user tables and generates its response accordingly.

To support the processing of realms the RADIUS server uses two special realms:

- Default realm: This realm is used where a realm is communicated for which no specific forwarding server has been defined. Significantly, a corresponding entry for the default realm itself needs to be present in the forwarding table.
- Empty realm: This realm is used when no realm is communicated, just the user name.

In the default state the forwarding table is empty, i.e. the default and empty realms are empty. This means that all requests are treated as local requests and any realms that are communicated are ignored. To operate the RADIUS server purely as a forwarding server or RADIUS proxy, set the default and empty realms to a value that corresponds to a server defined in the forwarding table.

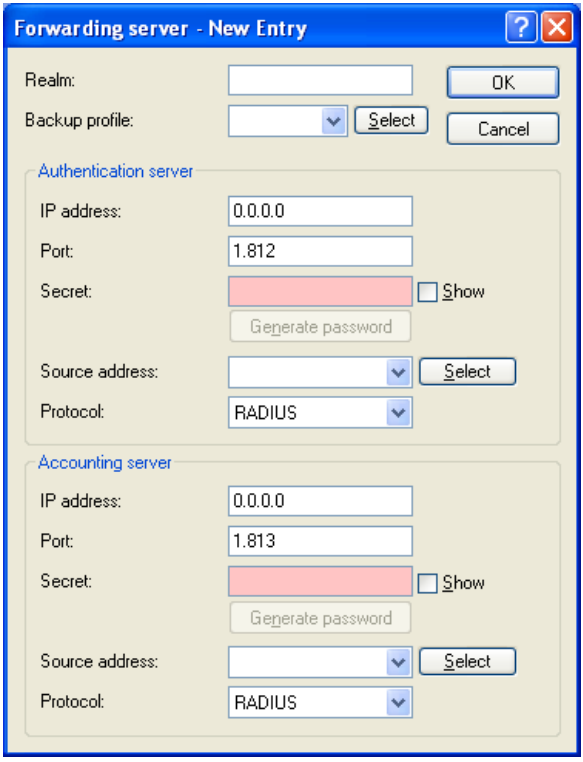
The forwarding of RADIUS requests does not alter the user name. No realm is added, changed or removed. The next server may not be the last one in the forwarding chain, and the realm information may be required by that server so that forwarding is carried out correctly. The active RADIUS server that processes the request resolves the realm from the user name, and subsequently a search is made of the table containing the user accounts. Accordingly the RADIUS server resolves the realm from the user name for processing requests locally.

The processing of tunneled EAP requests using TTLS and PEAP makes use of a special EAP tunnel server, which is also in the form of a realm. Here you select a realm that will not conflict with other realms. If no EAP tunnel server is defined then the RADIUS server forwards the request to itself, meaning that both the internal and the external EAP authentications are handled by the RADIUS server itself.

To configure RADIUS forwarding, create a list of forwarding servers, and define realms for this device, as follows:

☐ Navigate to the following dialog:`Configuration : RADIUS Server : Forwarding` and click "Forwarding server".

☐ In the ‘Forwarding server’ table, click ‘Add...’ to open the ‘New Entry’ dialog:



For each new forwarding server entry, configure the following parameters:

- Realm: Enter a string that defines the validity range of user accounts.
- Backup profile:
  Use this item to select the profile of an alternative forwarding server. Requests are forwarded to this server if the configured forwarding server is unavailable (see on page 350 „Chaining of Backup Servers“).
- IP address:
  Enter the IP address of the RADIUS Authentication server and/or the RADIUS accounting server you use for central user administration and/or central accounting.
- Port:
  Enter the port of the respective RADIUS server.

- Secret:
  Enter the key to be used as a Shared Secret.
- Source IP address:
  You have the option to enter a different address here (name or IP) to which the respective RADIUS server sends its reply message.
  By default, the server sends its replies back to the IP address of your device without having to enter it here. By entering an optional loopback address you change the source address and route used by the device to connect to the server. This can be useful, for example, when the server is available over different paths and it should use a specific path for its reply message.
- Protocol:
  Select the protocol for communication between the internal RADIUS server and the forwarding server: RADIUS or RADSEC.

Next, in the `Configuration : RADIUS Server : Forwarding` dialog, configure the following local RADIUS server parameters:

- ☐ Default-Realm: Enter the name of a realm that will be used if a realm is communicated for which no specific forwarding server has been defined. This realm needs to appear in the 'Forwarding server' table.
- ☐ Empty-Realm: Enter the name of the realm that will be used when no realm, just a user name, is communicated. This realm needs to appear in the 'Forwarding server' table.

WLAN Access List as a Basis for RADIUS Information

512 WLAN clients, that are able to register with the OpenBAT access point, may be entered in the access list. When operating in RADIUS server mode, this list can also be used to check on RADIUS clients that attempt to register at other access points. In an installation that includes several access points, this allows client access authorizations to be centrally maintained. The following settings for this configuration can be accessed at:

`HiLCOS menu tree : Setup : WLAN : RADIUS-Access-Check`

The following parameters can be configured for this purpose:

- **Provide server database:**
  This parameter specifies whether the WLAN access list is to be used as an information source for the RADIUS server in the OpenBAT access point. The WLAN access list contains the user name in the form of the MAC address and the password ('WPA passphrase'). In addition to this access data, the access list provides information such as bandwidth restriction and association to a specific VLAN.
- **Recheck cycle:**
  Enter a period, in minutes, to enable periodic checking of the client activity status. After a WLAN client is authenticated and logged on by RADIUS, it remains active until it logs off itself or is logged off by the RADIUS server. When you enter a value in this field, the RADIUS server periodically checks—at the specified period—whether the WLAN clients logged in are still in the access list. If a WLAN client is removed from the access list, it remains logged in to the WLAN up to the point when the recheck cycle runs again.

WPA Passphrase in the RADIUS Server User Table

The configuration of LEPS merely involves the assignment of an individual passphrase to the MAC address of each client that is approved for the WLAN. To this end, the MAC filter is set to positive, i.e. the data from clients entered here will be transmitted.

Note: The passphrases should consist of a random string at least 32 characters long.

The client-specific passphrase is stored in the RADIUS server's user table. This enables a device which is connected to the LAN to operate as a central RADIUS server and use the benefits of LEPS.

`HiLCOS Menu Tree:Setup:RADIUS:Server:Users:WPA passphrase`

14.9 RADSEC

RADSEC is an alternative protocol that transmits RADIUS packets through a TLS-encrypted tunnel. TLS is based on TCP, thus providing a proven mechanism for monitoring packet loss. Furthermore, TLS is highly secure and it features a method of mutual authentication by means of X.509 certificates.

14.9.1 Configuring RADSEC in the OpenBAT device

- The OpenBAT device as RADIUS client.

  To function as a RADIUS client, a OpenBAT device is set up to use RADIUS via UDP or RADSEC via TCP with TLS. Additionally set the port to be used. 1812 for authentication with RADIUS, 1813 for accounting with RADIUS, and 2083 for RADSEC.

  These settings are made at all locations in the WEBconfig software where a OpenBAT device is configured as a RADIUS client, including:

  `HiLCOS Menu Tree : Setup : WLAN : RADIUS`

  and

  `HiLCOS Menu Tree : Setup : WLAN : RADIUS Access Check`

  and

  `HiLCOS Menu Tree : Setup : WLAN : RADIUS Accounting`

  and

  `HiLCOS Menu Tree : Setup : IEEE802.1x : RADIUS Server`

The OpenBAT device as RADIUS server.

If a OpenBAT device operates as a RADIUS server, you can configure the RADSEC port for receiving RASDSEC logins. In addition to that, the protocol to be used (RADIUS, RADSEC or all) can be set for each of the RADIUS clients in the client list. This allows, for example, RADIUS to be used for LAN-based clients and the more robust RADSEC via TCP to be used for registrations arriving over the Internet.

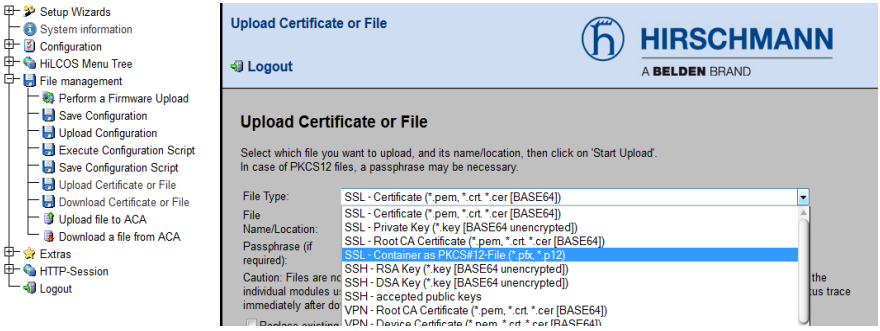
You can access and configure the ‘RADSEC port’ setting in LANconfig at:

☐ `Configuration : RADIUS Server : General`

14.9.2 Certificates for RADSEC

Separate X.509 certificates are required for TLS encryption of the RADSEC connection. The individual certificates (root certificate, devices certificate and private key) can be uploaded to the device individually or as a PKCS#12 container. This can be done at:

`File Management : Upload Certificate or File`



14.10TACACS+

14.10.1Introduction

TACACS+ (Terminal Access Controller Access-Control System Plus) is a protocol for authentication, authorization and accounting (AAA). It provides access to the network for authorized users, it regulates the rights of those users, and it is a logging mechanism to keep track of user actions. TACACS+ is an alternative to other AAA protocols such as RADIUS.

Note: Use TACACS+ in order to meet PCI (Payment Card Industry) compliance requirements.

Modern networks with their numerous types of service and network components present a challenge in terms of controlling access rights for the user. In large installations in particular, the overhead would be enormous to keep user data consistent on all devices or for all services. For this reason, user data should be managed on a central server.

As a simple example, a user wishes to register at a router and sends the corresponding login details (user ID) to it. In this case the router functions as a Network Access Server (NAS)—it does not check the user data itself; rather, the data is forwarded to the central AAA server, which responds by checking the data and answering with an „accept“ or a „reject“.

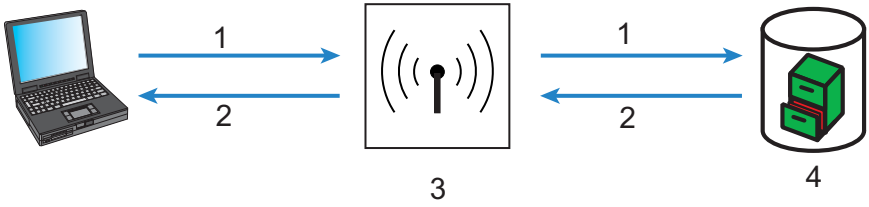


Figure 132:TACACS+ Network

1: User ID	3: NAS
2: Accept	4: AAA server

The advanced TACACS+ functions include, the option of requesting that users change their passwords after logging in for the first time, or if the password has expired. The corresponding messages are sent from the NAS to the user.

Note: LANconfig cannot process all of the messages in the extended login dialog. If LANconfig rejects a login attempt at a OpenBAT device even if the correct data is entered, use an alternative method of configuration (such as WEBconfig or Telnet).

TACACS+ is an alternative AAA server to RADIUS servers. The following table shows some of the major differences between RADIUS and TACACS+:

TACACS+	RADIUS
Connection-orientated data transfer via TCP	Connectionless data transfer via UDP
Fully encrypted data transfer	Password is encrypted, other content remains unencrypted
Complete separation of authentication, authorization and accounting possible	Authentication and authorization combined

- TCP-based communication with TACACS+ is more reliable with RADIUS. Communications between the NAS and AAA server are confirmed, so the NAS is informed if the AAA server is unavailable.
- TACACS+ encrypts the entire data payload (except for the TACACS+ header). This helps provide for the confidentiality of information such as user names or the permitted services. TACACS+ encryption works with a one-time pad based on MD5 hashes.
- The separation of the three AAA functions enables TACACS+ to operate with multiple servers. RADIUS combines authentication and authorization, TACACS+ allows these to be separated. In this way, for example, TACACS+ servers can be employed for authentication exclusively.

Note: Kindly note: Even if TACACS+ is used to centrally manage user accounts on an AAA server, you should by all means set a secure password for root access to the OpenBAT device. If no root password is set, access to the device configuration can be blocked to preserve security if no connection is available to the TACACS+ server. In this case, the device may have to be reset to its factory settings in order to regain access to the configuration.

14.10.2 Configuring TACACS+

The parameters for configuring TACACS+ can be accessed at:

`HiLCOS Menu Tree : Setup : TACACS+`

The following parameters can be configured:

- Accounting:
  Activates or deactivates accounting via TACACS+ server. If TACACS+ accounting is activated, all accounting data is transmitted via TACACS+ protocol to the configured TACACS+ server. Default = Deactivated.

  Note: TACACS+ accounting will activate provided the defined TACACS+ server is available.

- Authentication:
  Activates or deactivates authentication via TACACS+ server. If TACACS+ authentication is activated, all authentication data is transmitted via TACACS+ protocol to the configured TACACS+ server. Default = Deactivated.

  Note: TACACS+ authentication will activate only if an accessible TACACS+ server is defined. Fallback to local users is possible if a root password has been set for the OpenBAT device. Fallback to local users must be deactivated for devices without a root password, because otherwise access to the OpenBAT device without a password would be possible in case of a network failure (TACACS+ server not available).

- Authorization:
  Activates or deactivates authorization via TACACS+ server. If TACACS+ authorization is activated, all authorization data is transmitted via TACACS+ protocol to the configured TACACS+ server. Default = Deactivated.

  Note: TACACS+ authorization will activate provided the defined TACACS+ server is available. If TACACS+ authorization is activated, the TACACS+ server will be queried for authorization each time a user enters a command. Data traffic during configuration will increase correspondingly. Also, the user rights need to be defined in the TACACS+ server.

- Fallback to local users:
  If the defined TACACS+ server is unavailable, it is possible to fall back to local user accounts on the OpenBAT device. This allows for access to the device even if the TACACS+ connection is lost, e.g. when deactivating the usage of TACACS+ or for correcting the configuration. Default = Allowed.

Note: The fallback to local user accounts presents a security vulnerability if no root password is set for the OpenBAT device. For this reason, TACACS+ authentication with fallback to local user accounts can only be activated if a root password has been set. If no root password is set, access to the device configuration can be blocked for security reasons if a connection to the TACACS+ servers is unavailable. In this case, the device may have to be reset to its factory settings in order to regain access to the configuration.

- Shared secret:
  The password for encrypting the communications between NAS and TACACS+ servers, up to 31 alphanumeric characters.
- SNMP GET requests accounting:
  Numerous network management tools use SNMP for requesting information from network devices. LANmonitor also uses SNMP to access the OpenBAT device to display information about current connections, etc., or to execute actions such as disconnecting a connection. Since a device can also be configured via SNMP, TACACS+ evaluates these accesses as events that require authorization. Since LANmonitor regularly queries these values, a large number of unnecessary TACACS+ connections would be established. If authentication, authorization and accounting by TACACS+ are activated, then each request will initiate three sessions with the TACACS+ server.

  This parameter allows the regulation of the behavior of OpenBAT devices with regard to SNMP access in order to reduce the number of TACACS+ sessions required for accounting. Authentication via the TACACS+ server remains necessary if authentication for TACACS+ is activated generally.

  Note: Entering a read-only community enables authentication by TACACS+ to be deactivated for LANmonitor. The read-only community defined here is then entered into LANmonitor as a user name.

Values include:

- only_for_SETUP_tree (default): In this setting, accounting via the TACACS+ server is only required for SNMP access to the setup branch of HiLCOS.
- All: Accounting by TACACS+ server will be carried out for every SNMP access. In case of regular request for status information, for example, the load on the TACACS+ server will increase significantly.
- **None:**
  Accounting by TACACS+ server will not be carried out for SNMP accesses.

- SNMP GET requests authorization:
  This parameter allows the regulation of the behavior of OpenBAT devices with regard to SNMP access in order to reduce the number of TACACS+ sessions required for authorization. Authentication via the TACACS+ server remains necessary if authentication for TACACS+ is activated generally. Possible values:
  - only_for_SETUP_tree (default): In this setting, authorization via the TACACS+ server is only required for SNMP access to the setup branch of HiLCOS.
  - All: Authorization by TACACS+ server will be carried out for every SNMP access. In case of regular request for status information, for example, the load on the TACACS+ server will increase significantly.
  - None: Authorization by TACACS+ server will not be carried out for SNMP accesses.
- Bypass TACACS for CRON/scripts/action table:
  Select this to bypass TACACS+ for actions initiated by the CRON-Jobs table, the Action table, or configuration scripts. When selected, the OpenBAT device does not provide authorization or accounting messages for these actions.
- Encryption:
  Activates or deactivates the encryption of communications between NAS and TACACS+ servers. Default = Deactivated.

Note: For security reasons, operate TACACS+ with encryption. If encryption is activated here, the password for encryption entered here needs to match the password on the TACACS+ server.

- Include value into authorization request:
  Select this to require that both the configuration path and the parameter value need to be authorized by the TACACS+ Server, as in the following example:
  ```
  set /Setup/SNMP/Comment-1 "test"
  ```
  If this setting is de-selected, only the path needs to be authorized for the user, as in the following example:
  ```
  set /setup/SNMP/
  ```

14.10.3 Configuring the TACACS+ Server

Two servers can be defined to work with TACACS+ functions. One server acts as a backup in case the other one ceases to operate. When logging in via telnet or WEBconfig, the user can select the server to be used.

The parameters for configuring the TACACS+ server can be accessed at:

```
HiLCOS Menu Tree : Setup : TACACS+ : Server
```

The following parameters can be configured:

- Server address:
  Address of the TACACS+ server to which requests for authentication, authorization and accounting are to be forwarded. Values include any valid DNS resolvable name or valid IP address.
- Loopback address: (Optional)
  You can configure a loopback address here. Possible values include:
  – Name of the IP networks whose addresses are to be used
  – ‘INT’ for the address of the first intranet.
  – ‘DMZ’ for the address of the first DMZ

– LB0 to LBF for the 16 loopback addresses
– Any valid IP address

- Compatibility mode:
  Activated or deactivated. TACACS+ servers are available as open-source or commercial versions, each of which works with different messages. The compatibility mode enables the processing of messages from free TACACS+ servers. Default = Deactivated.

14.10.4Login to the TACACS+ Server

After TACACS+ has been activated for authentication and/or authorization, all logins to the device are redirected to the TACACS+ server. The remaining login procedure differs according to the access method.

TACACS+ Login via LANconfig

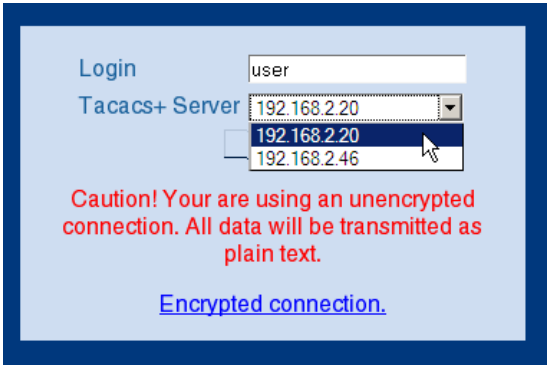
Using LANconfig to log in to a device with activated TACACS+ authentication requires the user named ‘root’. Correspondingly, the user ‘root’ needs to be configured on the TACACS+ server. To log in via LANconfig, enter the password as configured for the user ‘root’ on the TACACS+ server.

Note:

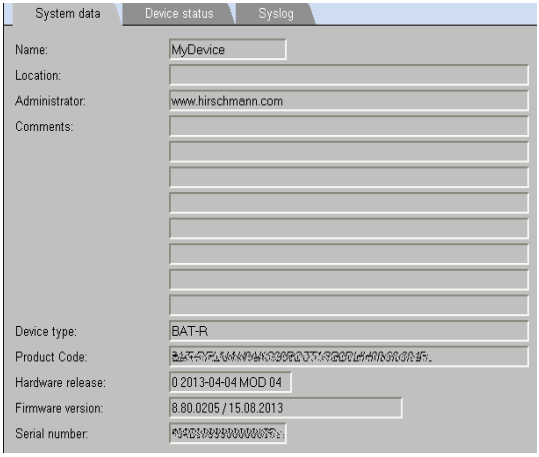
- After it is authenticated by TACACS+, ‘root’ is the sole user automatically assigned with full supervisor rights, and thus able to edit the configuration without having to change privilege level. When authorization is in use, the TACACS+ server decides whether this is allowed or not.
- If authorization is activated for the device as well as authentication, the TACACS+ server needs to permit the commands ‘readconfig’ and ‘writeconfig’ for the user ‘root’ in order for the user to read the configuration from the device and to upload any changes (see on page 940).

TACACS+ Login via WEBconfig

Using WEBconfig to log in to a device with activated TACACS+ authentication is possible for any user configured on the TACACS+ server. When logging in with WEBconfig, enter the user name configured on the TACACS+ server and select the server which is to carry out authentication:



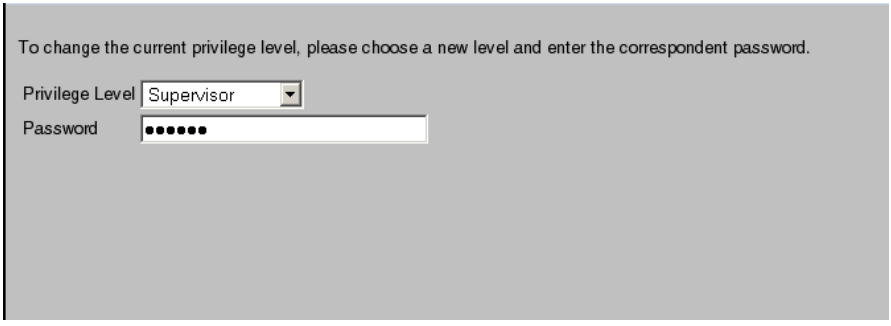
The corresponding password is requested in the following dialog. After logging in, the user initially sees a reduced WEBconfig user interface. If authorization is not being used, all WEBconfig users (except for the user ‘root’) initially have read rights exclusively.



To gain further rights, on the left of the screen click the following command:

`Change privilege level`

The following dialog opens where you can select the desired user rights and enter the corresponding password:

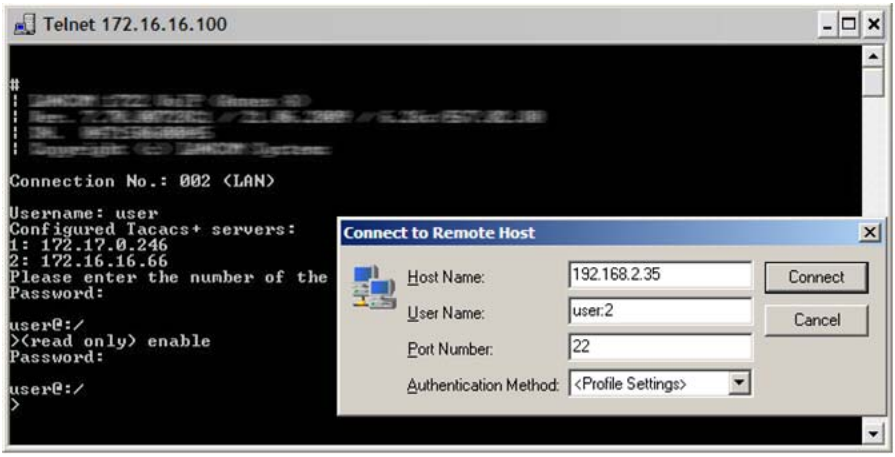

To change the current privilege level, please choose a new level and enter the correspondent password.
Privilege Level
Supervisor
Password
••••••

Note:

- The passwords for individual user rights are configured as "enable" passwords in the TACACS+ server.
- If authorization is activated for the device as well as authentication, the TACACS+ server needs to permit the assigned commands for each user in order for the user to read and edit the device configuration (see on page 940).

14.10.5TACACS+ Login via Telnet or SSH

Using Telnet or SSH to log in to a device with activated TACACS+ authentication is possible for any user configured on the TACACS+ server. When logging in with Telnet, enter the user name configured on the TACACS+ server and select the server which is to carry out authentication. When logging in with SSH, enter the user name followed by a colon and then the server name, i.e. "user:1" or "user:2".



After login, all users initially have read-only rights exclusively (except for the user ‘root’). To gain further rights, enter the command enable and enter the password. Rights will be assigned according to configuration for that password. The parameters for the enable command are the numbers 1-15. 1 is the lowest level, 15 the highest. If no parameter is entered, 15 is taken automatically.

Note:

- The passwords for individual user rights are configured as "enable" passwords in the TACACS+ server.
- If authorization is activated for the device as well as authentication, the TACACS+ server needs to permit the assigned commands for each user in order for the user to read and edit the device configuration (see on page 940).

14.10.6 Assigning Rights Under TACACS+

TACACS+ uses privilege levels to separate users into different groups. For the local authorization of users via the ‘enable’ command under telnet/SSH or via privilege levels under WEBconfig, the various administrator rights are mapped to the TACACS+ privilege levels:

TACACS+ level	Administrator rights
0	No rights
1	Read only
3	Read-write
5	Read-only limited admin
7	Read-write limited admin
9	Read only admin
11	Read-write admin
15	Supervisor (root)

14.10.7 Authorization Functions

If authorization is activated for the device as well as authentication, the TACACS+ server needs to permit the corresponding functions for the user. Enter the required values into the user configuration on the TACACS+ server.

- LANconfig

Command	Argument	Comment
readconfig	None	Read out the entire configuration
writeconfig	None	Write the entire configuration

- WEBconfig

Command	Argument	Comment
delRow	SNMP-ID of the table	Delete row
addrow	SNMP-ID of the table	Add row
editRow	SNMP-ID of the table	Edit row

Command	Argument	Comment
modifyItem	SNMP-ID of the menu item	Edit a menu item
viewTable	SNMP-ID of the table	View table
viewRow	SNMP-ID of the row	View row
setValue	SNMP-ID of the menu item	Set value of a menu item
listmenu	SNMP-ID of the menu	List sub menu
action	SNMP-ID of the action	Execute an action
reboot	None	Restart device
$URL	None	Display a certain URL

Note: For access via WEBconfig, all URLs sent to the TACACS+ server during configuration must be enabled. For example, the URL "config2" under WEBconfig provides access to the configuration branch of the Hirschmann menu tree. Additionally, the individual parameters that the user may edit also need to be enabled. You can view the URLs sent by WEBconfig to the TACACS+ server with the "trace+ tacacs" trace.

Telnet/SSH

Command	Argument	Comment
dir	SNMP-ID of the directory	View directory content
list	SNMP-ID of the directory	View directory content
ls	SNMP-ID of the directory	View directory content
llong	SNMP-ID of the directory	View directory content
del	SNMP-ID of the table	Delete row
delete	SNMP-ID of the table	Delete row
rm	SNMP-ID of the table	Delete row
cd	SNMP-ID of the target directory	Change directory
add	SNMP-ID of the table	Add row
tab	SNMP-ID of the table	Changes the order of the columns for adding value
do	SNMP-ID of the action	Execute action
show	Parameter name	View information
trace	Parameter name	Execute trace
time	Parameter name	Time
feature	Parameter name	Add function
repeat	Parameter name	Repeat the command
readmib	None	Read-out SNMP-MIB
readconfig	None	Read out the entire configuration
readstatus	None	Read-out status menu
writefiash	None	Update firmware
activateimage	Parameter name	Activate another firmware image
ping	Parameter name	Start ping

Command	Argument	Comment
wakeup	Parameter name	Sends wakeup packet
linktest	Parameter name	WLAN link test
writeconfig	None	Write the entire configuration
scp	Parameter name	Secure copy
rcp	Parameter name	Secure copy
readscript	Parameter name	Read-out script
beginscript	None	Start script
endscript	None	Stop script
flash	Parameter name	Activate/deactivate flash mod

Note: For telnet access, all of the parameters that the user may edit need to be enabled. You can view the values sent by telnet to the TACACS+ server with the trace ‘trace+ tacacs’.

SNMP

Command	Argument	Remark
get	SNMP-ID of the menu item	Read out value
set	SNMP-ID of the menu item	Set value

14.11 Support from TLS 1.1 / 1.2

The encryption protocols SSL and TLS (“Secure Sockets Layer” and “Transport Layer Security”) support secure data communication between 2 communication partners. This is effected by, for example, encrypting, authenticating and checking certificates that are sent. The protocol is mainly used to secure HTTP connections as “HTTPS” or “HTTP over SSL”. In addition, it is used by many other transmission protocols to provide secure communication.

HiLCOS uses the TLS protocol in the following modules:

- HTTP over SSL
- Telnet over SSL
- RADSEC
- CAPWAP/DTLS
- EAP-TLS/PEAP/TTLS

The TLS encryption protocol has developed from 1999 to the current version TLS 1.2. To use the corresponding enhanced functions of clients and Web browsers, Hirschmann devices support the current TLS protocol versions 1.0, 1.1 and 1.2 for secure data transmission.

All devices with HiLCOS versions before 8.60 use encryption protocols SSL 3.0 and TLS 1.0 as standard. From HiLCOS version 8.60 on, you have the option of selecting TLS versions 1.1 and 1.2.

A Glossary

802.11	WLAN specification of the IEEE; data rate up to 2 Mbit/s; in 2.4 GHz ISM band; FHSS and DSSS; infrared spectrum communications also planned
802.11a	Extension to 802.11; data rate up to 54 Mbit/s; in 5 GHz band; OFDM
802.11b	Extension to 802.11; data rate up to 11 Mbit/s; in 2.4 GHz band; high market penetration; DSSS/CCK
802.11g	Extension to 802.11; data rate up to 54 Mbit/s; in 2.4 GHz band; OFDM and DSSS
802.11h	802.11a customization, data rate up to 54 Mbit/s; in 5 GHz band; in area of transmission power and frequency management; for use in Europe; OFDM
802.11i	Future 802.11 extension with additional security features
802.11n	An improvement to 802.11 that adds multiple input/multiple output (MIMO) and other features.
802.11x	Specification of a port-based authentication mechanism from the IEEE.
AAA	Authentication, Authorization and Accounting
Access point (AP)	Base station in a WLAN; can be used in many different designs, including: ▶ connecting wireless communication client devices to either a WLAN or a wired LAN ▶ forming part of a wireless bridge connecting two wired LANs ▶ serving as a wireless bridge relay
Access router	Active network component for connection of a local network to the Internet or a company network.
ACL	Access Control List: a list of wireless stations that either may (whitelist) or may not (blacklist) access a wireless LAN.
ADSL	Asymmetrical Digital Subscriber Line – transmission process for high-speed data transmission over normal telephone lines. With ADSL, transmissions (downstream) of up to 6 Mbps can be implemented over normal telephone lines; for bidirectional transmission there is a second frequency band with transmission speeds of up to 640 kbps (upstream) - hence the name “asymmetric.”
AES	Advanced Encryption Standard; successor of DES.
ARF	Advanced Routing and Forwarding
ARP	Address Resolution Protocol
Bandwidth	Channel capacity or data rate through a communication path; the higher the bandwidth, the faster the connection.
Blowfish	A symmetric block cipher, eclipsed in popularity by AES.
BOOTP	Bootstrap Protocol
BPDU	Bridge Protocol Data Unit
Bridge	Transport protocol-independent, transparent network component; transmits all packets that are identified as “not local” and only understands the difference between “local” and “remote.” Works on Layer 2 of the OSI model.
Broadband	Service which provides high bandwidth; e.g.: DSL or WLAN

Broadcast	Broadcasts are packets to all stations of a local network; bridges transmit broadcasts; routers do not transmit broadcasts.
BSS	Basic Service Set
CAPI	Common ISDN Application Programming Interface - CAPI is a standard for control of ISDN adapters.
CBCP	Callback Control Protocol
CCK	Code Complementary Keying; type of modulation used by DSSS
CCP	Compression Control Protocol
CGI	Common Gateway Interface
Chaining	Concatenation of bit sequences.
CHAP	Challenge Handshake Authentication Protocol
Client	Common ISDN Application Programming Interface - CAPI is a standard for control of ISDN adapters.
CSD	Cyclic Shift Diversity
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance; access procedure to the radio channel used under 802.11.
CRC	Cyclic Redundancy Check; process for detecting inaccurate bit patterns.
CTS	Clear to send: Part of the RTS/CTS (Request to Send/Clear to Send) 802.11 function designed to help prevent an occurrence of the 'hidden station' phenomenon.
Data throughput	Speed at which you can send and receive data over a connection; depends on the bandwidth and the number of users
DDC	Direct Data Connect
DES	Data Encryption Standard: a form of shared secret encryption.
DFS	Dynamic Frequency Selection: a protocol for selecting only unused channels within a frequency, so as to avoid interference with radar systems.
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized Zone: a physical or logical subnetwork that exposes an organization's external services to an untrusted network.
DNS	Domain Name Server Computers communicate with one another in remote networks via IP addresses. DNS servers translate names into IP addresses. Without DNS servers you could only operate with IP addresses and not with names.
Domain	Area of network closed to outside => Intranet
DoS	Denial of Service
Download/ Downstream	Denotes the direction of dataflow in a WAN. Downstream is the direction from the head end or Internet to the participant connected to the network.
DPP	Dead Peer Protection
DS	Distribution System
DSCP	DiffServe code point: a 6-bit header in IP packets used to prioritize packets.
DSL	Digital Subscriber Line - DSL procedures include all procedures for digital-broadband use of telephone lines, such as ADSL, HDSL, SDSL, VDSL and so on, which are also called xDSL.
DSSS	Direct Sequence Spread Spectrum; code multiplex -- band spreading process
DTIM	Delivery Traffic Indication Message: a parameter for configuring beaconing.

DynDNS	Dynamic Domain Name System: IPsec-VPN implementation which allows the transparent connection of local networks into a VPN solution, even when their routers are working with dynamic addresses (dial-up).
EAP	Extensible Authentication Protocol
EAP-MD5	EAP variant which uses passwords for one-sided authentication.
EAP-TLS	EAP Transport Layer Security; EAP variant which uses certificates for mutual authentication.
EAP-TTLS	EAP Tunneled Transport Layer Security; EAP variant which uses certificates for mutual authentication.
EIRP	Effective Isotropic Radiated Power
ERP	Enterprise Resource Planning
ESS	Extended Service Set
ESSID	Extended Service Set Identity; “network name” of the wireless LAN.
Ethernet	The communication protocol defined by the IEEE as the 802.3 standard, Ethernet provides a wired access method for local area network (LAN) devices. The wireless version of Ethernet is WiFi.
FHSS	Frequency Hopping Spread Spectrum; frequency skipping band spread procedure.
Firewall	Protective mechanism for an Intranet against attacks from outside.
FQDN	Fully Qualified Domain Name
Frequency	Number of oscillations per second (given in Hertz; 1 Hz = 1 oscillation per second; GHz = Gigahertz = 1 billion Hertz or oscillations per second).
Frequency band	Contiguous frequency range which has the same transmission properties.
FTP	File Transfer Protocol: This protocol enables data transfer between different systems and simple file manipulation; FTP is based on the TCP transmission protocol.
FXP	File Exchange Protocol
Gateway	Network component which provides access to other network components on a layer of the OSI model. Packets which do not go to a local partner are sent to the gateway. The gateway takes care of communication with remote networks.
GPRS	General Packet Radio Service
HDLC	High-Level Data Link Control protocol
HiLCOS	Equivalent to Hirschmann operating system.
HotSpot	Locally limited wireless network with a base station with Internet access; public wireless Internet access.
HTTP	Hypertext Transfer Protocol
Hub	Network component; distributor; collector; also used to translate from one connection type to another.
IAPP roaming	Roaming between the cells of a wireless network using IAPP (Inter Access Point Protocol).
IBSS	Independent Basic Service Set
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System -- earliest possible detection of attacks on the network
IETF	Internet Engineering Task Force

IGMP	Internet Group Management Protocol
IMAP2	Internet Message Access Protocol version 2
Inband	The sending of control metadata—for example, parameter configuration values—on the same channel, or band, used for data.
IP Masquerading	Combination of PAT (Port Address Translation) and NAT (Network Address Translation) used for connection of an intranet (multiple workstations) to the Internet over a single IP address; simultaneously, the internal computers are shielded from attacks from outside.
IP Quality of Service	These functions give precedence to enterprise-critical applications, particular services, or user groups.
IPCP	Internet Protocol Control Protocol
IPSec	Internet Protocol Security
IPXCP	Inter-network Packet Exchange Control Protocol
IRC	Internet Relay Chat
ISDN	Integrated Services Digital Network -- fast connection; two independent channels; higher transmission rates than analog (up to 128 Kbit/s); uses the old analog lines; convenience features (call forwarding, callback on busy, etc.); supports both analog and digital services
ISM frequency band	Industrial-Scientific-Medical, license-free frequency bands which can be used for industrial, scientific, and medical purposes.
ISP	Internet Service Provider -- service provider with a connection to the Internet (backbone) who provides connection points for end customers.
IV	Initialization Vector
LAN	Local Area Network - local network limited to one site.
LANcapi	Virtual CAPI offered via the network. With LANcapi, which is implemented in all OpenBATs with an ISDN interface, a PC connected to the LAN can use ISDN telematic services.
LANconfig	Software for configuring OpenBATs in Windows.
LANmonitor	Software for monitoring LANs, consisting of OpenBATs in Windows.
LANtools	Extensive, user-friendly set of tools for the management and monitoring of OpenBAT devices, and related products and systems.
LCP	Link Control Protocol, part of the point-to-point (PPP) protocol.
LEPS	LANCOM Enhanced Passphrase Security
MAC	Media Access Control; radio access protocol on ISO Layer 2 data link; it defines packet format, packet addressing, and error detection.
MAC address	Serial number of a network component which is assigned by the manufacturer.
Mbit	Megabit: standard unit for the specification of data quantities in the context of bandwidths.
MCS	Modulation and Coding Scheme
MIC	Message Integrity Check, cryptographic integrity testing mechanism.
MS-CHAP	Microsoft version of Challenge Handshake Authentication Protocol
MTU	Maximum Transmission Unit
NAT	Network Address Translation
NBNS	NetBIOS Naming Service

NetBIOS	Network Basic Input/Output System. Non-routable network protocol for local networks developed by IBM and later taken over by Microsoft.
NNTP	Network News Transfer Protocol
NTBA	The NTBA (network termination basic adapter) is responsible in an ISDN base connection for the translation of the connection created by the telephone company to the S0 bus.
NTP	Network Time Protocol
OFDM	Orthogonal Frequency Division Multiplex
Outband	The sending of control metadata—for example, parameter configuration values—over a separate channel and not over the channel used for data.
P2MP	Point to multipoint: Multiple WLAN stations log into a base station and constitute a common network with the wired stations
P2P	Point to point: Two base stations connect two wired networks over WLAN; point-to-point operation enables coupling of networks even across streets without cables
PAP	Password Authentication Protocol
PCI	1. Peripheral component interconnect: a standardized bus for connecting peripheral components to the computer. 2. Payment Card Industry
PEAP	Protected EAP, EAP variant for mutual authentication
PKI	Public Key Infrastructure
PMK	Pairwise Master Key
PMTU	Path Maximum Transmission Unit
POP3	Post Office Protocol version 3
PPP	Point to Point Protocol: Network protocol for connecting two computers. PPP is based on TCP/IP.
PPPoE	Point-to-Point-Protocol over Ethernet: The protocol for encryption of PPP frames inside Ethernet frames.
PPTP	Point to Point Tunneling Protocol: Network protocol for the construction of virtual private networks over the Internet.
QoS	Quality of Service (see also IP Quality of Service)
Radio frequency	Every WLAN application uses globally regulated radio frequencies
RADIUS	Remote Authentication Dial-In User Service; authentication and monitoring protocol on the application level for authentication, integrity checking, and accounting for network access
RC4	Streaming cipher process by Ron Rivest, “Ron’s Code.”
RFC	Request for Comments
RIP	Routing Information Protocol
Router	Intelligent network component;, comparable to a post office, which can determine from the logical destination address of a packet which next network component should transmit the packet; knows the overall topology of the network.
RSA	An algorithm for public key cryptography, named for its inventors Rivest, Shamir and Adleman.
RSTP	Rapid Spanning Tree Protocol

RTS	Request to Send: Part of the RTS/CTS (Request to Send/Clear to Send) 802.11 function designed to help prevent an occurrence of the ‘hidden station’ phenomenon.
SDSL	Single Line Digital Subscriber Line - downstream and upstream at 2.048 Mbit/s (two-core cable).
Server	Computer which provides services over the network (e.g. files, news, email, WWW pages).
SINA	Secure Inter-Network Architecture
SMTP	Simple Mail Transfer Protocol - SMTP protocol is the Internet standard for distribution of electronic mail; the protocol is based on the TCP protocol.
SNMPv3	Simple Network Management Protocol Version 3
SPI	Stateful Packet Inspection
SSH	Secure shell
SSID	Service Set Identity; “network name” of the wireless LAN.
SSL	Secure Socket Layer
Splitter	The splitter is comparable to an audio frequency filter; in an ADSL connection, the splitter separates the ISDN signals from the DSL signals; the ISDN signals go to the NTBA and the DSL signals go to the DSL modem
STP	Spanning Tree Protocol
Switch	A central distributor in a network that connects network segments. A switch sends data packets on the OSI Data Link Layer (Layer 2). The switch can also carry out this task on the OSI Network Layer (Layer 3). Switches are used to reduce collision, thereby increasing the overall throughput of the network.
SYN/ACK	Synchronization/acknowledge
SYSLOG	A standard for logging program messages—it allows for separation of the program that generates the message from the program that analyzes the messages.
TACACS+	Terminal Access Controller Access-Controller System Plus: A proprietary protocol for controlling accesses – such as authentication, authorization and accounting – to network devices.
TAE	Telephone connection unit used in Germany. Plug for the connection of analog devices like a telephone or modem into the telephone network.
TCP/IP	Transmission Control Protocol/Internet Protocol; family of protocols (ARP, ICMP, IP, UDP, TCP, HTTP, FTP, TFTP) used mainly in the Internet, although it is making headway in intranets as well.
Telnet	TELE NETwork: a protocol providing bi-directional, text-based, interactive communication.
TFTP	Trivial File Transfer Protocol
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
TPC	Transmission Power Control
TTLS	Transport Layer Security
TU	Timer Unit: a time unit of measure for the IEEE 802.1 standard, equal to 1 k?s.
UDP	User Datagram Protocol: one of the core protocols of the IP suite that enable unconnected messaging.

Upload/Upstream	Upload/upstream denotes the direction of dataflow in a WAN; upstream is the direction from the node connected to the network to the head end/ Internet
URL	Uniform Resource Locator
USB	Universal Serial Bus
VLAN	Virtual Local Area Network
VoIP	Voice over Internet Protocol: a group of technologies for the transmission of voice communications over IP.
VPN	Virtual Private Network: a VPN is a network consisting of virtual connections over which non-public or company internal data can be transmitted securely, even if public network infrastructures are used.
WAN	Wide Area Network: network connection over long distances (e.g., via ISDN with a OpenBAT).
WDS	Wireless Distribution System
WECA	Wireless Ethernet Compatibility Alliance: alliance of manufacturers of wireless LAN components based on IEEE 802.11; renamed the WiFi Alliance.
WEBconfig	Web-based configuration interface for OpenBATs.
WEP	Wired Equivalent Privacy
WiFi	wireless fidelity; marketing term promulgated by the WECA. WiFi is defined by IEEE as the 802.11 standard and is the wireless counterpart to wired Ethernet.
WiFi-Alliance	Wireless Ethernet Compatibility Alliance: alliance of manufacturers of wireless LAN components based on IEEE 802.11; renamed the WiFi Alliance.
WISP	Wireless Internet Service Provider
WLAN	Wireless Local Area Network
WME	Wireless Multimedia Extensions
WMM	WiFi Multimedia
WPA	WiFi Protected Access; name for security mechanisms beyond IEEE 802.11; generated by the WiFi Alliance.
WPA2	Successor to WPA.
WLAN	Wireless Local Area Network - local radio network
xDSL	xDSL stands for the family of Digital Subscriber Line technologies.
XOR	Logical operation “exclusive OR”

B Index

Numerics

802.11 945
802.11a 945
802.11b 945
802.11g 945
802.11h 945
802.11i 945
802.11n 945
802.11x 945

A

AAA 945
Access Point 27, 29
Access point 945
Access Point example
  DHCP server 78
Access point example
  basic settings 51
  configuration file 48
  configuring DHCP WLAN 82
  configuring the LAN 79
  WLAN settings 59
Access restricted 513
  by IP address 516
  by source 514
Access router 945
Accounting 883
ACL 945
Action table 652
  configuring 658, 661
  dynamic DNS 652
Address translation configuration 597
ADSL 945
AES 945
ARF 521, 560, 568, 945
ARP 945

B

Background WLAN scanning 509
Bandwidth 945
  granted minimum 837
Blowfish 945
Boot images list 853
BOOTP 847, 945
BPDU 945
Bridge 945
Bridge group 282
Broadband 945
Broadcast 946
Brute force attack 513
BSS 946

C

Callback 621
  CBCP 622
  configuring 622, 624
  fast 623
  Other Router 624
  PPP LCP 624
CAPI 946
CAPWAP data tunnel 277
CAPWAP standard
  Control channel 273
  Data channel 273
  Data-channel advantages 274
  Payload data 274
  Transmission channels 273
CBCP 622, 946
CCK 946
CCP 946
CGI 946
Chaining 946
CHAP 946
Client 946
COM port adapters 680
COM port server 665
  byte counters 678
  COM port errors 679
  COM port status 677
  configuring 667
  connections 679
  device ports table 668
  network interface table 671
  network status 676
  operating modes 666
  serial interface table 669

status 676
Communication layers list 576
Configuration
download 41
offline 40
online 40
Software 37
Configuration file
create by copying 79, 132, 156, 178
creating 44
CRC 946
CRON table 896
CSD 946
CSMA/CA 946
CTS 946

D

Data throughput 946
Daylight savings time 894
DDC 946
DES 946
Device
configuration 43
roles 27
Device operating state table 675
Device ports table 668
DFS 946
DHCP 946
vendor class and user class ID 868
DHCP network table 858
DHCP networks table 863
configuring 848
DHCP relay 847
DHCP relay server 863
DHCP server 846
additional options 861
alias list 857
assign client boot image 854
assign client IP address 854
boot image list 857
configuring 848
configuring via Telnet 855
configuring via WEBconfig 855
create a boot image 853
DHCP status table 862
enable/disable by logical interface 848
hosts table 857
IGMP packet data 856
networks list 858
port table 861
relay server 863
DHCP table 866
DiffServ 833
firewall rules 835
VLAN 529
DMZ 587, 946
assignment of network zones to 588
multiple IP address design 590
separation from intranet LANs 590
unmasked internet access 589
DNS 846, 869, 946
dynamic 880, 947
forwarding 871
URL blocking 879
DNS server
configuring 873
Domain 946
DoS 739, 946
Download 946
Download configuration 41
Downstream 946
DS 946
DSCP 946
DSL 946
DSL connection
limiting call charges 886
DSSS 946
DTIM 946
Dynamic DNS 947

E

EAP 919, 947
EAP-MD5 947
EAP-TLS 947
EAP-TTLS 947
EIRP 947
ERP 947
ESS 947
ESSID 947
Ethernet 947
Example of an Access Point 47

F

FAQ 967
Fast callback 623
FHSS 947
Firewall 947
action objects 722
action table 727
actions 708

and masked connections 705
configuration tips 698
configuring 701
connection list 732
creating new filter rule 706
default setting 698
defining objects 720
denial of service (DoS) attacks 739
diagnosing 728
DoS configuration 739
e-mail event notification 702
enable/disable 702
filter list 730
FTP 717
host block list 734
HTML configuration 724
intrusion detection system (IDS) 736
IRC 717
limitations 735
log table 728
Network Address Translation (NAT) 699
objects table 725
packet fragments 702
ping blocking 704
port block list 733
QoS objects 722
rule settings 708
rules table 724
service objects 723
session recovery 702
station objects 723
stealth mode 704
Firewall strategies
deny all 699
FQDN 947
Frequency 947
band 947
FTP 947
FXP 947

G

Gateway 947
GPRS 947
backup connection 630
Granted minimum bandwidths 837

H

HDLC 947
HiLCOS 947
HotPlug-capable adapters 675
Hotpluggable adapters 666
HotSpot 947
Hub 947
HyperTerminal 37

I

IAPP roaming 947
IBSS 947
ICMP 947
redirects 550
IDS 736, 947
address checking 589
configuring 737
IETF 947
IGMP 948
IGMP snooping 681
configuring 687
multiple bridges 684
operation 683
status 692
IMSP2 948
Inverse IP masquerading 582
IP address assignment to PC in Windows 865
IP Masquerading 948
IP masquerading 579
and stateful inspection 584
configuring 581
inverse 582
transmittable protocols 581

IP networks table 566
IP QoS 948
IP routing 542
IPCP 948
IPSec 948
IPXCP 948
IRC 948
ISDN 948
ISM frequency band 948
ISP 590, 948
IV 948

K

Keep-Alive-Functionn 620

L

LAN 948
LANcapi 948
LANconfig 948
LANmonitor 948
LANtools 948
Layer-3 roaming 284
LCP 948
  PPP connection checking 603
LEPS 508, 948
Login lock 513

M

MAC 948
MAC address 948
Mbit 948
MCS 948
MIC 948
Modem
  serial interface 626
MS-CHAP 948
MTU 638, 948
  configuring 638
  statistics 639

N

NAT 591, 699, 948
  address translation 597
  network coupling 591, 592
  remote monitoring/control 591, 593
NAT table 597
NBNS 948
NetBIOS 846, 949
NetBIOS proxy 572
Network
  assigning interfaces 566
  defining 566
Network coupling 591, 592
Network interface table 671
Network separation
  Application example 279
Networks
  separating 277
NNTP 949
NTBA 949
NTP 891, 949

O

OFDM 949
Offline configuration 40
Online configuration 40
Overlay network 274, 277
  Configuration public spot 287

P

PAP 949
Password
  SNMP read 512
Password configuring 512
Payload data
  Forwarding from WLANs 284
PCI 929, 949
PEAP 949
Peer list 624
Ping blocking 704
PKI 949
PMK 949
PMTU 949
Point-to-multipoint 949
Point-to-point 949
Point-to-point (1 subnet) example
  WLAN settings 114
Point-to-point (2 subnets) example
  creating a transfer network 145
  routing the transfer network 150
Point-to-point example
  (1 subnet)
    basic settings 106
Point-to-point example (1 subnet) 105
Point-to-point example (2 subnets) 142
Point-to-point relay (1 radio) example
  configure master 167
  configure slave 161, 172
Point-to-point relay (2 radios) example
  configure master 179
  configure slave 191, 194

Point-to-point relay example (1 radio) 155
Point-to-point relay example (2 radios) 177
Poisoned reverse 558
Polling table 635
POP3 949
Port forwarding table 584
Port mapping 584
Port table 567, 861
PPP 600, 949
application scenarios 601
assigning IP addresses 604
configuring 606
description 600
negotiation phases 602
RADIUS authentication 609
PPP list 606, 609
PPPoE 608, 611
configuring 615
example application 612
limited to subnet 611
PPTP 548, 949
DSL dial-in 617
PPTP list 617
Public spot
WLAN Controller 287

Q

QoS 831, 948, 949
enabled/disabled 834
objective 832
Reducing packet length 839
Transmission and reception direction 838
WLANs 842

R

Radio frequency 949
Radio interface
default setting 39
RADIUS 609, 900, 949
802.1x client access 910
access list 925
accounting 904
client configuring 927
operation 902
PPP client access 905
server configuring 928
versus TACACS+ 930
WLAN client access 908
X.509 certificates 928
RADIUS Server
Add clients 915
RADIUS server
adding users 915
configuring 912
EAP authentication 919
forwarding 922
general settings 913
RC4 949
Remote site
configuring 574
Remote site (peer) list 574
Remote sites (serial) list 633, 634
RFC 949
RIP 551, 949
configuring 553
configuring filter 554
for separate networks 555
LAN triggered update 557
poisoned reverse 558
static routes 558
WAN triggered update 557
RIP filter 554
RIP table 553
Roaming
Application example 286
Layer-3 284
Roles 27
Router 949
Routing 539, 542
Advanced 560
assign WAN interface tags 569
assignment of network zones to DMZ 588
DMZ 587
dynamic 551
ICMP redirects 550
IP masquerading 579
NAT 591
NetBIOS proxy 572
network definition 566
on the LAN 550
policy based 546
port mapping 584
PPP 600
PPTP connection tags 548
remote site confguring 574
routing vs. interface tags 564
SYN/ACK speedup 559

virtual router 570
virtual routers 568
VPN connection tags 548
Routing table 542
configuring 543
IP masquerading setup 581
RSA 949
RSTP 643, 949
configuring 646
enable/disable 646
statistics 648
versus STP 644
RTS 950

S

SDSL 950
Separation of networks 277
Serial interface
backup connection 634
Configuration 666
configuring for modem 628
modem operation 626
remote site connection 633
statistics 631
trace output 632
Serial interface table 669
Server 950
Session recovery 702
Setup wizard
access point basic settings 52
access point WLAN settings 59
Check security settings 510
point-to-point basic settings 106
point-to-point WLAN settings 114
wireless client basic settings 89
wireless client WLAN settings 94
Silent rejection
TCP and UDP packets 704
SINA 950
SMTP 950
SNMP 37
read password 512
SNMPv3 950
SPI 950
Splitter 950
SSH 950
SSID 950
SSL 950
STP 950
Switch 950
Symbol 25
SYSLOG 950
System requirements 627

T

Table Clients 915
Table Forwarding server 923
TACACS+ 929
assigning rights 940
authorization functions 940
configuring 931
server configuring 935
server login (LANconfig) 936
server login (Telnet/SSH) 939
server login (WEBconfig) 937
versus RADIUS 930
TAE 950
TCP packet
silent rejection 704
TCP/IP 950
Technical Questions 967
Telnet 37, 950
modem command 631
TFTP 37, 950
Time server 889
configuring 889
configuring clients 891
Time zone 892
TKIP 507, 950
TLS 927, 950
ToS 833
VLAN 529
TPC 950
Training Courses 967
TTLS 950
TU 950

U

UDP 950
UDP packet
silent rejection 704

Upload 951
Upstream 951
URL 951
USB 951
User table 915

V

Virtual router 570
Virtual routers 568
VLAN 951
  ARF 521
  assigning clients 527
  configuring 521
  define 523
  description 520
  enable/disable 522
  general settings 522
  port configuration 524
  special DSL IDs 528
  tags on layers 2/3 529
VoIP 951
VPN 951

W

WAN 951
  connections 539
  functions 540
WAN RIP table
  configuring 640
WAN tag table 569
WDS 951
WEBconfig 951
WECA 951
WEP 951
WiFi 951
WiFi-Alliance 951
Windows
  assigning IP address to a PC 865
Wireless client example
  creating configuration file 85
WISP 951
WLAN 951
  default settings 39
WLAN Bridge 27
  Point-to-Point 30
WLAN bridge example
  WLAN settings 114
WLAN Bridge Relay 27
WLAN bridge relay 32
WLAN Client 28, 34
WLAN Client example 85
WLAN Controller 277
  Public spot 287
WLAN Distribution Point 27
WLAN distribution point
  point-to-multipoint 33
WLAN profile 281
WLAN roaming client 28, 35
WLAN settings 280
WLC interfaces (virtual) 275
WLC tunnel 275, 280
WME 842, 951
WMM 842, 951
WPA 507, 951
WPA2 507, 951

X

xDSL 951
XOR 951

C General Information

C.1 Maintenance

Hirschmann is continually working to improve and develop our software. You should regularly check whether there is a new version of the software that provides you with additional benefits. You will find software information and downloads on the product pages of the Hirschmann website.

C.2 Readers' Comments

What is your opinion of this manual? We are constantly striving to provide as comprehensive a description of our product as possible, as well as important information to assist you in the operation of this product. Your comments and suggestions help us to further improve the quality of our documentation.

Your assessment of this manual:

	Very Good	Good	Satisfactory	Mediocre	Poor
Precise description	O	O	O	O	O
Readability	O	O	O	O	O
Understandability	O	O	O	O	O
Examples	O	O	O	O	O
Structure	O	O	O	O	O
Comprehensive	O	O	O	O	O
Graphics	O	O	O	O	O
Drawings	O	O	O	O	O
Tables	O	O	O	O	O

Did you discover any errors in this manual?
If so, on what page?

General Information

Suggestions for improvement and additional information:

General comments:

Sender:

Company / Department:

Name / Telephone number:

Street:

Zip code / City:

E-mail:

Date / Signature:

Dear User,

Please fill out and return this page

- as a fax to the number +49 (0)7127/14-1600 or
- per mail to

  Hirschmann Automation and Control GmbH
  Department 01RD-NT
  Stuttgarter Str. 45-51
  72654 Neckartenzlingen

D Further Support

Technical Questions

For technical questions, please contact any Hirschmann dealer in your area or Hirschmann directly.

You will find the addresses of our partners on the Internet at http://www.hirschmann.com

Contact our support at https://hirschmann-support.belden.eu.com

You can contact us

in the EMEA region at
- Tel.: +49 (0)1805 14-1538
- E-mail: hac.support@belden.com

in the America region at
- Tel.: +1 (717) 217-2270
- E-mail: inet-support.us@belden.com

in the Asia-Pacific region at
- Tel.: +65 6854 9860
- E-mail: inet-ap@belden.com

Hirschmann Competence Center

The Hirschmann Competence Center is ahead of its competitors:

- Consulting incorporates comprehensive technical advice, from system evaluation through network planning to project planning.
- Training offers you an introduction to the basics, product briefing and user training with certification.
  The current technology and product training courses can be found at http://www.hicomcenter.com
- Support ranges from the first installation through the standby service to maintenance concepts.

With the Hirschmann Competence Center, you have decided against making any compromises. Our client-customized package leaves you free to choose the service components you want to use.
Internet:
http://www.hicomcenter.com

HIRSCHMANN

A BELDEN BRAND